
Amazon Elastic Compute Cloud

Manual do usuário para instâncias do Windows



Amazon Elastic Compute Cloud: Manual do usuário para instâncias do Windows

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens de marcas da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigue a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, conectados ou patrocinados pela Amazon.

Table of Contents

O que é o Amazon EC2	1
Recursos do Amazon EC2	1
Como começar a usar o Amazon EC2	2
Serviços relacionados	2
Acessar o Amazon EC2	3
Definição de preço do Amazon EC2	4
Conformidade do PCI DSS	4
Configurar	6
Cadastre-se no AWS	6
Criar um par de chaves	6
Crie um grupo de segurança	7
Tutorial de conceitos básicos	10
Overview	10
Prerequisites	11
Etapa 1: executar uma instância	11
Etapa 2: conectar-se à instância	12
Etapa 3: limpar a instância	18
Próximas etapas	18
Práticas recomendadas	19
Imagens de máquina da Amazon	22
Modos de inicialização	22
Considerations	23
Requisitos para executar uma instância com UEFI	23
Determinar o parâmetro de modo de inicialização de uma AMI	24
Determinar os modos de inicialização suportados por um tipo de instância	25
Determinar o modo de inicialização de uma instância	25
Determinar o modo de inicialização do sistema operacional	26
Definir o modo de inicialização de uma AMI	26
AWSAMIs do Windows	29
Selecionar uma AMI inicial do Windows	30
Manter suas AMIs atualizadas	30
Tipos de virtualização	30
AMIs do Windows gerenciadas pela AWS	30
Criar uma AMI do Windows personalizada	39
Cancelar o registro da AMI do Windows	55
AMIs especializadas do Windows	56
AWSHistórico de versões da AMI do Windows da	62
Localizar uma AMI do Windows	102
Localizar uma AMI do Windows usando o console do Amazon EC2	103
Localizar uma AMI usando o AWS Tools for Windows PowerShell	104
Localizar uma AMI usando o AWS CLI	104
Localizar a AMI do Windows mais recente usando o Systems Manager	105
Use um parâmetro de Systems Manager para localizar uma AMI	105
AMIs compartilhadas	108
Encontrar AMIs compartilhadas	108
Tornar um AMI pública	110
Compartilhar uma AMI com contas específicas da AWS	112
Usar marcadores	114
Melhores práticas para AMIs compartilhadas do Windows	115
AMIs pagas	115
Vender sua AMI	116
Localizar uma AMI paga	116
Comprar uma AMI paga	118
Obter o código do produto para sua instância	118

Usar suporte pago	118
Faturas para AMI pagas e compatíveis	119
Gerenciar suas assinaturas do AWS Marketplace	119
Ciclo de vida da AMI	120
Criar uma AMI	120
Copiar um AMI	120
Armazenar e restaurar uma AMI	126
Defasjar uma AMI	132
Automatizar o ciclo de vida da AMI com suporte do EBS	135
Usar criptografia com AMIs com EBS	135
Cenários de execução de instância	136
Cenários de cópia de imagem	138
Noções básicas sobre o faturamento da AMI	140
Campos de faturamento da AMI	141
Localizar informações de faturamento de AMI	142
Verificar cobranças da AMI em sua fatura	144
Instâncias	145
Instâncias do Windows	145
Instâncias e AMIs	145
Diferenças entre o Windows Server e instâncias do Windows	146
Projetar suas aplicações para serem executadas em instâncias do Windows	148
Tipos de instância	149
Tipos de instâncias disponíveis	149
Especificações de hardware	153
Instâncias criadas no Sistema Nitro	154
Recursos de redes e armazenamento	155
Limites de instâncias	158
Propósito geral	158
Otimizadas para computação	204
Otimizado para memória	211
Otimizada para armazenamento	222
Computação acelerada	228
Localizar um tipo de instância do	242
Alterar o tipo de instância	244
Obter recomendações	249
Opções de compra de instância	253
Determinar o ciclo de vida da instância	254
On-Demand Instances	255
Reserved Instances	259
Instâncias programadas	298
Spot Instances	299
Dedicated Hosts	349
Dedicated Instances	383
On-Demand Capacity Reservations	390
Ciclo de vida da instância	412
Execução da instância	413
Interrupção e início de instância (somente instâncias baseadas no Amazon EBS)	414
Hibernação de instância (somente instâncias baseadas no Amazon EBS)	414
Reinicialização da instância	415
Desativação da instância	415
Encerramento de instância	415
Diferenças entre reinicialização, interrupção, hibernação e encerramento	416
Executar	417
Conecte-se	443
Interromper e iniciar	455
Hibernar	459
Reinicializar	470

Retirada	471
Encerrar	474
Recuperar	480
Configurar instâncias	482
EC2Launch v2	482
EC2Launch	522
Serviço EC2Config	530
Drivers de PV	559
AWSDrivers NVMe	580
Otimizar as opções de CPU	582
Definir o horário	601
Definir a senha	605
Adicionar componentes do Windows	606
Configurar um endereço IPv4 privado secundário	610
Executar comandos na inicialização	614
Metadados da instância e dados do usuário	622
Clustering do SQL Server no EC2	670
Atualizar instâncias do Windows	676
Realizar uma atualização no local	677
Realizar uma atualização automatizada	681
Migrar para tipos de instância da geração mais recente	688
Migrar o Microsoft SQL Server do Windows para o Linux	694
Solucionar problemas de uma atualização	702
Identificar instâncias do	702
Inspecione o documento de identidade da instância	702
Inspecione o UUID do sistema	702
Configurar um cluster do Windows HPC	703
Prerequisites	703
Etapa 1: Criar seus grupos de segurança	704
Etapa 2: Configurar o controlador de domínio do Active Directory	706
Etapa 3: Configurar o nó do cabeçalho	707
Etapa 4: Configurar o nó de computação	709
Etapa 5: Dimensione seus nós de computação de HPC (opcional)	710
Frotas	712
EC2 Fleet	712
Limitações da Frota do EC2	713
Instâncias expansíveis	713
Tipos de solicitação da Frota do EC2	714
Estratégias de configuração da Frota do EC2	732
Trabalhar com Frotas do EC2	741
Frota spot	761
Tipos de solicitação da frota spot	761
Estratégias de configuração de frota spot	761
Trabalhar com frotas spot	769
Métricas do CloudWatch para frota spot	790
Escalabilidade automática para frota spot	792
Monitorar eventos da frota	799
Tipos de evento de Frota do EC2	799
Tipos de evento de frota spot	803
Criar uma regra de EventBridge	808
Tutoriais	813
Tutorial: Usar a Frota do EC2 com ponderação de instâncias	814
Tutorial: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal	816
Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas	817
Tutorial: Usar frota spot com ponderação de instâncias	822
Exemplos de configuração	824
Exemplos de configuração de Frota do EC2	824

Exemplos de configuração de frota spot	837
Quotas da frota	848
Elastic Graphics	850
Conceitos básicos de Elastic Graphics	850
Definição de preço do Elastic Graphics	852
Limitações de Elastic Graphics	852
Como trabalhar com o Elastic Graphics	852
Configurar grupos de segurança	853
Iniciar uma instância com uma aceleradora do Elastic Graphics	854
Instalar o software necessário para o Elastic Graphics	855
Verificar a funcionalidade do Elastic Graphics em sua instância	855
Ver informações do Elastic Graphics	857
Enviar feedback	858
Usar métricas do CloudWatch para monitorar o Elastic Graphics	858
Métricas do Elastic Graphics	858
Dimensões do Elastic Graphics	859
Visualizar métricas do CloudWatch para o Elastic Graphics	859
Criar alarmes do CloudWatch para monitorar o Elastic Graphics	860
Troubleshoot	860
Investigar problemas na performance da aplicação	860
Resolver problemas de status não íntegros	862
Monitor	864
Monitoramento automático e manual	865
Ferramentas de monitoramento automatizadas	865
Ferramentas de monitoramento manual	866
Melhores práticas de monitoramento	867
Monitorar o status das instâncias	867
Verificações de status de instâncias	867
Eventos agendados	874
Monitorar instâncias usando o CloudWatch	898
Habilitar o monitoramento detalhado	899
Listar métricas disponíveis	901
Obter estatísticas para métricas	914
Representar métricas em gráficos	922
Criar um alarme	922
Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância	924
Automatizar o Amazon EC2 com o EventBridge	936
Registrar em log as chamadas de APIs com o AWS CloudTrail	937
Informações sobre o Amazon EC2 e o Amazon EBS no CloudTrail	937
Noções básicas sobre entradas dos arquivos de log no Amazon EC2 e no Amazon EBS.	938
Auditar usuários que se conectam por EC2 Instance Connect	939
Monitorar as aplicações .NET e SQL Server	940
Redes	942
Regiões e zonas	942
Regions	943
Zonas de disponibilidade	947
Local Zones	949
Zonas do Wavelength	953
AWS Outposts	955
Endereçamento IP de instâncias	956
Endereços IPv4 privados e nomes de host DNS internos	956
Endereços IPv4 públicos e nomes de host DNS externos	957
Endereços IP elásticos (IPv4)	958
Servidor DNS da Amazon	958
Endereços IPv6	958
Trabalhar com os endereços IPv4 para as instâncias	959
Trabalhar com os endereços IPv6 para as instâncias	962

Vários endereços IP	964
Traga seus próprios endereços IP	972
Requisitos e cotas	973
Configurar seu intervalo de endereços BYOIP	973
Trabalhar com o intervalo de endereços	980
Saiba mais	981
Atribuição de prefixos	981
Noções básicas para atribuição de prefixos	982
Considerações e limites para prefixos	982
Trabalhar com prefixes	983
Endereços IP elásticos	993
Definição de preço de endereços IP elásticos	993
Noções básicas sobre endereços IP elásticos	993
Trabalhar com endereços IP elásticos	994
Usar DNS reverso para aplicações de e-mail	1000
Limite de endereços IP elásticos	1001
Interfaces de rede	1002
Conceitos básicos da interface de rede	1002
Endereços IP por interface de rede por tipo de instância	1004
Trabalhar com interfaces de rede	1015
Cenários para interfaces de rede	1023
Melhores práticas para configurar interfaces de rede	1025
Interfaces de rede gerenciadas pelo solicitante	1025
Largura de banda de rede	1026
Largura de banda disponível da instância	1027
Monitorar largura de banda da instância	1028
Redes avançadas	1028
Suporte a redes avançadas	1029
Habilitar redes avançadas na instância	1029
Redes avançadas: ENA	1029
Rede avançada: Intel 82599 VF	1037
Otimizações do sistema operacional	1040
Métricas de performance da rede	1041
Grupos de posicionamento	1044
Placement groups de cluster	1044
Placement groups de partição	1045
Placement groups de distribuição	1046
Regras e limitações do placement group	1047
Criar um placement group	1048
Marcar um placement group	1049
Executar instâncias em um placement group	1051
Descrever instâncias em um placement group	1052
Alterar o placement group de uma instância	1054
Excluir um placement group	1055
Conexão MTU	1056
Frames jumbo (9.001 MTU)	1057
Path MTU Discovery	1057
Verificar o MTU do caminho entre dois hosts	1058
Verificar e definir o MTU na instância do Windows	1058
Troubleshoot	1060
Nuvens privadas virtuais	1060
Documentação da Amazon VPC	1060
Portas e protocolos	1061
Roteador AllJoyn	1061
Cast para dispositivo	1062
Redes de núcleos	1064
Otimização de entrega	1088

Trilha de Diag	1089
Servidor de protocolo DIAL	1089
Gerenciamento Distributed File System (DFS)	1089
Compartilhamento de arquivos e impressora	1090
Gerenciamento remoto do servidor de arquivos	1094
Todos os ICMP v4	1094
Multicast	1095
Desktop Remoto	1095
Gerenciamento de dispositivos do Windows	1097
Gerenciamento remoto de Firewall do Windows	1098
Gerenciamento remoto do Windows	1099
EC2-Classic	1099
Detectar plataformas suportadas	1099
Tipos de instância disponíveis no EC2-Classic	1101
Diferenças entre instâncias no EC2-Classic e em uma VPC	1101
Compartilhar e acessar recursos entre EC2-Classic e uma VPC	1106
ClassicLink	1107
Migre do EC2-Classic para uma VPC	1119
Segurança	1129
Segurança da infraestrutura	1130
Isolamento de rede	1130
Isolamento em hosts físicos	1130
Controlar o tráfego de rede	1130
VPC endpoints de interface	1132
Criar um VPC endpoint de interface	1132
Criar uma política de VPC endpoint de interface	1132
Resiliência	1133
Proteção de dados	1134
Criptografia em repouso	1135
Criptografia em trânsito	1135
Identity and Access Management	1137
Acesso à rede para a instância	1137
Atributos de permissões do Amazon EC2	1137
IAM e Amazon EC2	1138
Políticas do IAM	1139
AWSPolíticas gerenciadas pela	1194
Funções do IAM	1195
Acesso à rede	1205
Pares de chaves	1209
Criar um par de chaves usando o Amazon EC2	1210
Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2	1211
Etiquetar uma chave pública	1213
Recuperar a chave pública da chave privada	1214
Recuperar a chave pública por meio de metadados de instância	1215
Identificar o par de chaves que foi especificado na execução	1215
Verificar a impressão digital do par de chaves	1215
Excluir o par de chaves	1216
Conectar-se à instância do Windows se você perder a chave privada	1217
Grupos de segurança	1217
Regras de grupos de segurança	1218
Acompanhamento da conexão	1220
Grupos de segurança padrão e personalizados	1222
Trabalhar com grupos de segurança	1223
Regras de grupo de segurança para diferentes casos de uso	1233
Gerenciamento de configuração	1238
Gerenciamento de atualizações	1239

Gerenciamento de alterações	1239
Validação de conformidade	1239
Auditoria e responsabilidade	1240
Storage	1242
Amazon EBS	1243
Recursos do Amazon EBS	1244
Volumes do EBS	1245
Snapshots do EBS	1294
Amazon Data Lifecycle Manager	1363
Serviços de dados do EBS	1409
Volumes do EBS e NVMe	1438
Otimização de EBS	1440
Performance do EBS	1458
Métricas do CloudWatch para o EBS	1472
CloudWatch Events para EBS	1479
Cotas do EBS	1490
Armazenamento de instâncias	1490
Vida útil do armazenamento de instâncias	1491
Volumes de armazenamento de instâncias	1492
Adicionar volumes de armazenamento de instâncias	1499
Volumes de armazenamento de instâncias SSD	1503
Armazenamento de arquivos	1504
Amazon S3	1504
Amazon EFS	1506
Amazon FSx	1506
Limites de volumes de instância	1507
Limites de volumes do Sistema Nitro	1507
Limites de volumes específicos do Windows	1507
Largura de banda x capacidade	1508
Volume do dispositivo raiz	1508
Configurar o volume raiz para persistir	1508
Confirmar que um volume raiz está configurado para persistir	1510
Alterar o tamanho inicial do volume raiz	1511
Nomes de dispositivos	1512
Nomes de dispositivos disponíveis	1512
Considerações sobre nomes de dispositivos	1513
Mapeamentos de dispositivos de blocos	1513
Conceitos de mapeamento de dispositivos de blocos	1514
Mapeamento de dispositivos de blocos da AMI	1517
Mapeamento de dispositivos de blocos de instância	1519
Mapear discos para volumes	1524
Listar volumes do NVMe	1524
Listar volumes	1528
Implantar o Storage Spaces Direct	1533
Etapa 1: Executar e ingressar instâncias no domínio	1536
Etapa 2: Instalar e configurar os pré-requisitos de instâncias	1538
Etapa 3: Criar cluster de failover	1540
Etapa 4: Habilitar o S2D	1540
Etapa 5: Provisionar o armazenamento	1541
Etapa 6: Rever os recursos do S2D	1541
Etapa 7: Limpeza	1542
Recursos adicionais	1543
Recursos e tags	1544
Localizações de recursos	1544
IDs de recursos	1545
Listar e filtrar seus recursos	1546
Listar e filtrar recursos usando o console	1547

Listar e filtrar usando a CLI e a API	1551
Listar e filtrar recursos entre Regiões usando o Amazon EC2 Global View	1553
Marcar com tag os recursos do	1554
Conceitos básicos de tags	1554
Marcar com tag os recursos do	1555
Restrições de tags	1558
Gerenciamento de tags e acesso	1559
Marcar com tag recursos para faturamento	1559
Trabalhar com tags usando o console	1560
Trabalhar com tags usando a linha de comando	1563
Adicionar tags a um recurso usando o CloudFormation	1566
Cotas de serviço	1567
Visualizar os limites atuais	1567
Solicitar um aumento	1568
Restrição para e-mails enviados usando a porta 25	1568
Relatórios de uso	1569
Solução de problemas	1570
Solucionar problemas de execução	1570
Limite de instâncias excedido	1570
Capacidade insuficiente da instância	1571
A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis.	1571
A instância é encerrada imediatamente	1572
Alto uso de CPU logo após o início do Windows	1573
Conecte-se à sua instância	1573
O Remote Desktop não pode se conectar ao computador remoto	1574
Erro ao usar o cliente RDP do macOS	1576
O RDP exibe uma tela preta em vez da área de trabalho	1577
Não foi possível fazer login remotamente em uma instância com uma conta de usuário que não é de administrador	1577
Resolução de problemas do desktop remoto usando o AWS Systems Manager	1577
Habilitar a área de trabalho remota em uma instância do EC2 com registro remoto	1580
Solucionar problemas de uma instância não acessível	1581
Obter uma captura de tela de uma instância inacessível	1581
Capturas de tela comuns	1582
Redefinir uma senha de administrador do Windows perdida ou expirada	1590
Redefinir com o EC2Launch v2	1591
Redefinir usando o EC2Config	1594
Redefinir usando o EC2Launch	1598
Parar a instância	1602
Forçar a parada da instância	1602
Para criar uma instância de substituição	1603
Encerrar a instância	1605
A instância é encerrada imediatamente	1605
Encerramento atrasado da instância	1605
Instância encerrada ainda sendo exibida	1605
Instâncias executadas ou encerradas automaticamente	1605
Solucionar problemas do Sysprep	1605
EC2Rescue for Windows Server	1606
Usar a GUI	1607
Usar a linha de comando	1611
Usar o Systems Manager	1616
Console serial do EC2	1618
Configurar o acesso ao console serial do EC2	1619
Conectar-se ao console serial do EC2	1624
Encerrar uma sessão do console serial do EC2	1628
Solucionar problemas da instância usando o console Serial do EC2	1629

Enviar uma interrupção para diagnóstico	1633
Tipos de instâncias compatíveis	1634
Prerequisites	1634
Enviar uma interrupção para diagnóstico	1634
Problemas comuns	1634
Os volumes do EBS não são inicializados no Windows Server 2016 e posterior	1635
Inicialize uma instância do EC2 Windows no Directory Services Restore Mode (DSRM)	1635
A instância perde a conectividade de rede ou as tarefas agendadas não são executadas quando esperado	1637
Não foi possível obter o resultado do console	1638
Windows Server 2012 R2 não disponível na rede	1638
Mensagens comuns	1638
"A senha não está disponível"	1639
"A senha ainda não está disponível"	1639
"Não é possível recuperar a senha do Windows"	1639
"Esperando o serviço de metadados"	1640
"Não é possível ativar o Windows"	1642
"O Windows não é genuíno (0x80070005)"	1644
"Nenhum servidor de licença do servidor terminal disponível para fornecer uma licença"	1644
"Algumas configurações são gerenciadas pela sua organização"	1645
AWS Systems Manager para Microsoft System Center VMM	1646
Features	384
Limitations	129
Requirements	1647
Conceitos básicos	1647
Configurar	1647
Cadastre-se no AWS	1647
Configurar o acesso para usuários	1648
Implantar o suplemento	1650
Forneça suas credenciais da AWS	1650
Gerenciar instâncias do EC2	1651
Criar uma instância do EC2	1651
Visualizar suas instâncias	1654
Conecte-se à sua instância	1654
Reinicializar a instância	1655
Parar a instância	1655
Executar sua instância	1655
Encerrar a instância	1655
Importar sua VM	1656
Prerequisites	1656
Importar sua máquina virtual	1656
Verificar o status da tarefa de importação	1657
Fazer backup de sua instância importada	1658
Solução de problemas	1658
Erro: Não é possível instalar o suplemento	1658
Erros de instalação	1659
Verificar o arquivo de log	1659
Erros ao importar uma máquina virtual	1659
Desinstalar o suplemento	1660
AWS Management Pack	1661
Visão geral do AWS Management Pack para o System Center 2012	1661
Visão geral do AWS Management Pack para o System Center 2007 R2	1663
Baixar	1664
System Center 2012	1664
System Center 2007 R2	1665
Implantação	1665
Etapa 1: Instalar o AWS Management Pack	1666

Etapa 2: Configurar o nó observador	1667
Etapa 3: Criar uma conta Executar como da AWS	1668
Etapa 4: Executar o Assistente para Adicionar monitoramento	1672
Etapa 5: Configurar portas e endpoints	1676
Use	1676
Views	1677
Discoveries	1691
Monitors	1692
Rules	1693
Events	1693
Modelo de integridade	1694
Personalizar o AWS Management Pack	1696
Upgrade	1697
System Center 2012	1697
System Center 2007 R2	1697
Desinstalar	1698
System Center 2012	1698
System Center 2007 R2	1698
Solução de problemas	1698
Erros 4101 e 4105	1699
Erro 4513	1699
Evento 623	1699
Eventos 2023 e 2120	1699
Evento 6024	1700
Solução de problemas em geral do System Center 2012 — Operations Manager	1700
Solução de problemas em geral para o System Center 2007 R2	1701
Informações relacionadas	1702
Histórico do documento	1704
História dos anos anteriores	1712

O que é o Amazon EC2?

O Amazon Elastic Compute Cloud (Amazon EC2) oferece uma capacidade de computação escalável na Nuvem da Amazon Web Services (AWS). O uso do Amazon EC2 elimina a necessidade de investir em hardware inicialmente, portanto, você pode desenvolver e implantar aplicativos com mais rapidez. É possível usar o Amazon EC2 para executar quantos servidores virtuais forem necessários, configurar a segurança e as redes e gerenciar o armazenamento. O Amazon EC2 permite aumentar ou reduzir a escala para lidar com alterações nos requisitos ou com picos em popularidade, reduzindo sua necessidade de prever o tráfego.

Para obter mais informações sobre computação em nuvem, consulte [What is cloud computing? \(O que é computação em nuvem?\)](#).

Recursos do Amazon EC2

O Amazon EC2 fornece os seguintes recursos:

- Ambientes de computação virtual, conhecidos como instâncias
- Os modelos pré-configurados para suas instâncias, conhecidos como Imagens de máquina da Amazon (AMIs), que empacotam os bits de que você precisa para seu servidor (incluindo o sistema operacional e software adicional)
- Várias configurações de capacidade de CPU, memória, armazenamento e redes para suas instâncias, conhecidas como tipos de instância
- Informações seguras de login para suas instâncias usando pares de chave (a AWS armazena a chave pública e você armazena a chave privada em um lugar seguro)
- Volumes de armazenamento para dados temporários que são excluídos quando você interrompe, hiberna ou encerra sua instância, conhecidos como volumes de armazenamento de instâncias
- Volumes de armazenamento persistentes para seus dados usando o Amazon Elastic Block Store (Amazon EBS), conhecidos como volumes do Amazon EBS
- Vários locais físicos para seus recursos, como instâncias e volumes do Amazon EBS, conhecidos como regiões e zonas de disponibilidade
- Um firewall que permite especificar os protocolos, portas e intervalos de IPs de origem que podem acessar suas instâncias usando grupos de segurança
- Os endereços IPv4 estáticos para computação em nuvem dinâmica, conhecidos como endereços IP elásticos
- Metadados, conhecidos como tags, que você pode criar e atribuir aos recursos do Amazon EC2
- Redes virtuais isoladas logicamente do restante da Nuvem AWS que você pode criar e, opcionalmente, conectar à sua própria rede, conhecida como nuvens virtuais privadas (VPCs)

Para obter mais informações sobre os recursos do Amazon EC2, consulte a [página do produto Amazon EC2](#).

O Amazon EC2 permite que você execute qualquer solução compatível baseada em Windows em nossa plataforma de alta performance, confiável e econômica de computação em nuvem. Para obter mais informações, consulte [Windows Server na AWS](#).

Para obter mais informações sobre como executar seu site na AWS, consulte [Web Hosting](#) (Hospedagem na Web).

Como começar a usar o Amazon EC2

Primeiro, você precisa fazer é configurar o Amazon EC2 para ser usado. Após a configuração, você estará pronto para concluir o tutorial de conceitos básicos do Amazon EC2. Sempre que você precisar de mais informações sobre um recurso do Amazon EC2, poderá ler a documentação técnica.

Comece já

- [Configuração para usar o Amazon EC2. \(p. 6\)](#)
- [Tutorial: Comece a usar instâncias Windows do Amazon EC2 \(p. 10\)](#)

Basics

- [Instâncias do Windows do Amazon EC2 \(p. 145\)](#)
- [Tipos de instância \(p. 149\)](#)
- [Tags \(p. 1554\)](#)

Redes e segurança

- [Pares de chaves \(p. 1209\)](#)
- [Grupos de segurança \(p. 1217\)](#)
- [Endereços IP elásticos \(p. 993\)](#)
- [Nuvens privadas virtuais \(p. 1060\)](#)

Storage

- [Amazon EBS \(p. 1243\)](#)
- [Armazenamento de instâncias \(p. 1490\)](#)

Trabalhar com instâncias do Windows

- [AWS Systems Manager Run Command](#) (Run Command do AWS Systems Manager) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).

Se você tiver dúvidas sobre se a AWS é adequada para você, [entre em contato com Vendas da AWS](#). Se você tiver dúvidas técnicas sobre o Amazon EC2, use o [fórum do Amazon EC2](#).

Serviços relacionados

Você pode provisionar recursos do Amazon EC2, como instâncias e volumes, usando diretamente o Amazon EC2. Você pode provisionar os recursos do Amazon EC2 usando outros serviços na AWS. Para obter mais informações, consulte a documentação a seguir:

- [Guia do usuário do Amazon EC2 Auto Scaling](#)
- [AWS CloudFormation Guia do usuário](#)
- [AWS Elastic Beanstalk Guia do desenvolvedor do](#)

- [AWS OpsWorks Guia do usuário](#)

Para distribuir automaticamente o tráfego de entrada de aplicativos entre várias instâncias, use o Elastic Load Balancing. Para obter mais informações, consulte o [Elastic Load Balancing User Guide](#) (Guia do usuário do Elastic Load Balancing).

Para obter um banco de dados relacional gerenciado na nuvem, use o Amazon Relational Database Service (Amazon RDS) para executar uma instância de banco de dados. Embora você possa configurar um banco de dados em uma instância do EC2, o Amazon RDS oferece a vantagem de lidar com suas tarefas de gerenciamento de banco de dados, como correção de software, backup e armazenamento de backups. Para obter mais informações, consulte o [Amazon Relational Database Service Developer Guide](#) (Guia do desenvolvedor do Amazon Relational Database Service).

Para facilitar o gerenciamento de contêineres do Docker em um cluster de instâncias do EC2, use o Amazon Elastic Container Service (Amazon ECS). Para obter mais informações, consulte o [Amazon Elastic Container Service Developer Guide](#) (Guia do desenvolvedor do Amazon Elastic Container Service) ou o [Amazon Elastic Container Service User Guide for AWS Fargate](#) (Guia do usuário do Amazon Elastic Container Service para AWS Fargate).

Para monitorar as estatísticas básicas de suas instâncias e volumes do Amazon EBS, use o Amazon CloudWatch. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch](#).

Para detectar o uso potencialmente não autorizado ou mal-intencionado de suas instâncias do EC2, use o Amazon GuardDuty. Para obter mais informações, consulte [Amazon GuardDuty User Guide](#) (Guia do usuário do Amazon GuardDuty).

Acessar o Amazon EC2

O Amazon EC2 fornece uma interface de usuário na web, o console do Amazon EC2. Depois de cadastrar-se em uma conta da AWS, você pode acessar o console do Amazon EC2 fazendo login no AWS Management Console e selecionando EC2 na página inicial do console.

Se preferir usar uma interface de linha de comando, temos as seguintes opções:

AWSInterface da linha de comando (CLI)

Fornece comandos para um conjunto amplo de produtos da AWS e é compatível com Windows, Mac e Linux. Para começar a usar, consulte o [AWS Command Line Interface User Guide](#) (Guia do usuário da AWS Command Line Interface). Para obter mais informações sobre comandos para o Amazon EC2, consulte [ec2](#) na AWS CLI Command Reference (Referência de comandos da AWS CLI).

AWS Tools for Windows PowerShell

Fornece comandos para um conjunto amplo de produtos da AWS para os usuários que usam script no ambiente do PowerShell. Para começar a usar, consulte o [AWS Tools for Windows PowerShell User Guide](#) (Guia do usuário do AWS Tools for Windows PowerShell). Para obter mais informações sobre os cmdlets do Amazon EC2, consulte a [AWS Tools for PowerShell Cmdlet Reference](#) (Referência de cmdlets do AWS Tools for Windows PowerShell)

O Amazon EC2 permite a criação de recursos usando o AWS CloudFormation. Você cria um modelo, em JSON ou YAML, que descreve seus recursos da AWS e o AWS CloudFormation provisiona e configura esses recursos para você. Você pode reutilizar seus modelos do CloudFormation para provisionar os mesmos recursos várias vezes, seja na mesma região e conta ou em várias regiões e contas. Para obter mais informações sobre os tipos de recurso e as propriedades do Amazon EC2, consulte [EC2 resource type reference](#) (Referência de tipo de recurso do EC2) no AWS CloudFormation User Guide (Guia do usuário do AWS CloudFormation).

A Amazon EC2 fornece uma API de consulta. Essas são solicitações HTTP ou HTTPS que usam verbos HTTP GET ou POST e um parâmetro de consulta chamado `Action`. Para obter mais informações sobre as ações de API para o Amazon EC2, consulte [Ações](#) no Amazon EC2 API Reference.

Se você preferir criar aplicativos usando APIs específicas de uma linguagem em vez de enviar uma solicitação via HTTP ou HTTPS, a AWS fornece bibliotecas, código de exemplo, tutoriais e outros recursos para desenvolvedores de software. Essas bibliotecas fornecem funções básicas que automatizam tarefas, como assinatura criptografada de suas solicitações, novas tentativas de solicitações e tratamento das respostas de erro, facilitando para que você comece rapidamente. Para obter mais informações, consulte [Ferramentas para criar na AWS](#).

Definição de preço do Amazon EC2

Ao se cadastrar na AWS, você poderá começar a usar o Amazon EC2 gratuitamente usando o [Nível gratuito da AWS](#).

O Amazon EC2 fornece as seguintes opções para comprar instâncias:

On-Demand Instances

Pague pelas instâncias que você usar por hora, sem nenhum compromisso a longo prazo nem pagamentos adiantados.

Savings Plans

É possível reduzir os custos do Amazon EC2 se comprometendo com uma quantidade consistente de uso, em USD por hora, por um período de vigência de um ou de três anos.

Reserved Instances

É possível reduzir os custos do Amazon EC2 se comprometendo com uma configuração específica de instância, incluindo o tipo de instância e a região, por um período de vigência de um ou de três anos.

Spot Instances

Solicite instâncias do EC2 não utilizadas, o que pode reduzir os custos do Amazon EC2 significativamente.

Para obter uma lista completa de cobranças e preços do Amazon EC2, consulte [Definição de preço do Amazon EC2](#).

Para calcular o custo de um exemplo de ambiente provisionado, consulte [Centro de informações sobre economia da nuvem](#).

Para ver sua fatura, acesse o Painel de gerenciamento de custos e faturamento no [console do AWS Billing and Cost Management](#). Sua fatura contém links para relatórios de uso que fornecem detalhes sobre sua conta. Para saber mais sobre o faturamento da conta da AWS, consulte o [AWSGuia do usuário do Billing and Cost Management](#).

Se tiver dúvidas sobre faturamento, contas e eventos da AWS, [entre em contato com o Suporte da AWS](#).

Para obter uma visão geral do Trusted Advisor, um serviço que ajuda você a aperfeiçoar os custos, a segurança e a performance do ambiente da AWS, consulte [AWS Trusted Advisor](#).

Conformidade do PCI DSS

O Amazon EC2 é compatível com o processamento, o armazenamento e a transmissão de dados de cartão de crédito por um comerciante ou um provedor de serviços e foi validada como em conformidade

com o Data Security Standard (DSS, Padrão de segurança de dados) da Payment Card Industry (PCI, Padrão de cartão de crédito). Para obter mais informações sobre o PCI DSS, incluindo como solicitar uma cópia do pacote de conformidade com o PCI da AWS, consulte [Nível 1 do PCI DSS](#).

Configuração para usar o Amazon EC2.

Conclua as tarefas nesta seção para configurar a execução de uma instância do Amazon EC2 pela primeira vez:

1. Cadastre-se no AWS (p. 6)
2. Criar um par de chaves (p. 6)
3. Crie um grupo de segurança (p. 7)

Quando terminar, você estará pronto para o tutorial [Conceitos básicos do Amazon EC2 \(p. 10\)](#).

Cadastre-se no AWS

Quando você se cadastra na Amazon Web Services, a conta da AWS é cadastrada automaticamente em todos os produtos da AWS, incluindo o Amazon EC2. Você será cobrado apenas pelos serviços que usar.

Com o Amazon EC2, você paga somente pelo que for usado. Se você for um cliente novo da AWS, poderá começar a usar o Amazon EC2 gratuitamente. Para obter mais informações, consulte [Nível gratuito da AWS](#).

Se já tiver uma conta da AWS, passe para a próxima tarefa. Se você ainda não possuir uma conta da AWS, use o procedimento a seguir para criar uma.

Para criar uma conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções online.

Parte do procedimento de cadastro envolve uma chamada telefônica e a digitação de um código de verificação usando o teclado do telefone.

Criar um par de chaves

AWS usa criptografia de chave pública para proteger as informações de logon da instância. Você especifica o nome do par de chaves ao iniciar a instância e fornece a chave privada para obter a senha de administrador para a sua instância do Windows para que você possa fazer login usando RDP.

Se ainda não tiver criado um par de chaves, você poderá criar um usando o console do Amazon EC2. Observe que, se quiser iniciar instâncias em várias regiões, você precisará criar um par de chaves em cada região. Para obter mais informações sobre regiões, consulte [Regiões e zonas \(p. 942\)](#).

Como criar o par de chaves

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Key Pairs (Pares de chaves).

3. Escolha Create key pair (Criar par de chaves).
4. Em Name (Nome), insira um nome descritivo para o par de chaves. O Amazon EC2 associa a chave pública ao nome especificado como o nome da chave. Um nome de chave pode incluir até 255 caracteres ASCII. Não pode incluir espaços no início nem no final.
5. Para o tipo de par de chaves, escolha RSA ou ED25519. Note que as chaves ED25519 não são compatíveis com instâncias do Windows, EC2 Instance Connect ou Console de série do EC2.
6. Para Formato de arquivo de chave privada, escolha o formato no qual salvar a chave privada. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha pem. Para salvar a chave privada em um formato que possa ser usado com o PuTTY, escolha ppk.

Se você escolheu ED25519 na etapa anterior, o formato de arquivo de chaves privadas não aparece, e o formato de chave privada é o padrão PEM.

7. Escolha Create key pair (Criar par de chaves).
8. O arquivo de chave privada é baixado automaticamente pelo navegador. O nome do arquivo base é o nome especificado como o nome do par de chaves e a extensão do nome do arquivo é determinada pelo formato do arquivo escolhido. Salve o arquivo de chave privada em um lugar seguro.

Important

Esta é a única chance de você salvar o arquivo de chave privada.

Para obter mais informações, consulte [Pares de chaves do Amazon EC2 e instâncias do Windows \(p. 1209\)](#).

Crie um grupo de segurança

Os security groups atuam como firewall para instâncias associadas, controlando o tráfego de entrada e de saída no nível da instância. Você deve adicionar regras a um grupo de segurança que permita a conexão com a instância em seu endereço IP usando RDP. Você também pode adicionar regras que permitam o acesso HTTP e HTTPS de entrada e saída de qualquer lugar.

Para executar instâncias em várias regiões, você precisa criar um grupo de segurança em cada região. Para obter mais informações sobre regiões, consulte [Regiões e zonas \(p. 942\)](#).

Prerequisites

Você precisará do endereço IPv4 público do computador local. O editor do grupo de segurança no console do Amazon EC2 pode detectar automaticamente o endereço IPv4 público para você. Como alternativa, você pode usar a frase de pesquisa "qual é meu endereço IP" em um navegador de Internet ou o serviço a seguir: [Verificar IP](#). Caso esteja se conectando por meio de um Internet Service Provider (ISP – Provedor de serviços de Internet) ou atrás de um firewall sem um endereço IP estático, você precisa descobrir o intervalo de endereços IP usados por computadores cliente.

É possível criar um grupo de segurança personalizado usando um dos métodos a seguir.

New console

Para criar um security group com o menor privilégio

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação superior, selecione uma Região para o grupo de segurança. Os grupos de segurança são específicos para uma região, portanto, você deve selecionar a mesma região em que criou o par de chaves.
3. No painel de navegação esquerdo, escolha Security Groups.

4. Escolha Create security group (Criar grupo de segurança).
5. Em Basic details (Detalhes básicos), faça o seguinte:
 - a. Insira um nome para o novo security group e uma descrição. Escolha um nome que seja fácil de lembrar, como o nome de usuário, seguido por _SG_, mais o nome da região. Por exemplo, me_SG_uswest2.
 - b. Na lista VPC selecione sua VPC padrão para a região.
6. para oRegras de entradaCrie regras que permitem que um tráfego específico alcance sua instância. Por exemplo, use as seguintes regras para um servidor Web que aceite tráfego HTTP e HTTPS. Para obter mais exemplos, consulte [Regras de grupo de segurança para diferentes casos de uso \(p. 1233\)](#).
 - a. Escolha Adicionar regra. Para Tipo, escolha HTTP. Para Source (Origem), escolha Anywhere (Qualquer lugar).
 - b. Escolha Adicionar regra. Para Type, escolha HTTPS. Para Source (Origem), escolha Anywhere (Qualquer lugar).
 - c. Escolha Add rule (Adicionar regra). Em Type (Tipo), escolha RDP. Em Source (Origem), siga um dos seguintes procedimentos:
 - Escolha My IP (Meu IP) para adicionar automaticamente o endereço IPv4 público do computador local.
 - Como alternativa, escolha Custom e especifique o endereço IPv4 público do computador ou da rede em notação CIDR. Para especificar um único endereço IP em notação CIDR, adicione o prefixo de roteamento /32, por exemplo, 203.0.113.25/32. Se sua empresa alocar endereços de um intervalo, especifique o intervalo inteiro, como 203.0.113.0/24.

Warning

Por motivos de segurança, não escolha Qualquer lugar para Origem com uma regra para RDP. Isso permitiria o acesso à sua instância a partir de todos os endereços IP na Internet. Isso é aceitável por um período curto em um ambiente de teste, mas não é seguro em ambientes de produção.

7. para oRegras de saídaManter a regra padrão, que permite todo o tráfego de saída.
8. Escolha Create security group (Criar grupo de segurança).

Old console

Para criar um security group com o menor privilégio

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação esquerdo, escolha Security Groups.
3. Escolha Create Security Group.
4. Insira um nome para o novo security group e uma descrição. Escolha um nome que seja fácil de lembrar, como o nome de usuário, seguido por _SG_, mais o nome da região. Por exemplo, me_SG_uswest2.
5. Na lista VPC selecione sua VPC padrão para a região.
6. Na guia Regras de entrada, crie as seguintes regras (escolha Adicionar regra para cada nova regra):
 - Selecione HTTP na lista Tipo e verifique se Origem está definida como Qualquer lugar (0.0.0.0/0).
 - Selecione HTTPS na lista Tipo e verifique se Origem está definida como Qualquer lugar (0.0.0.0/0).

- Escolha RDP na lista Type. Na caixa Source, escolha My IP para preencher automaticamente o campo com o endereço IPv4 público do computador local. Como alternativa, escolha Custom e especifique o endereço IPv4 público do computador ou da rede em notação CIDR. Para especificar um único endereço IP em notação CIDR, adicione o prefixo de roteamento /32, por exemplo, 203.0.113.25/32. Se sua empresa alocar endereços de um intervalo, especifique o intervalo inteiro, como 203.0.113.0/24.

Warning

Por motivos de segurança, não permita RDP acesso de todos os endereços IP à instância. Isso é aceitável por um período curto em um ambiente de teste, mas não é seguro em ambientes de produção.

7. Na guia Regras de saída, mantenha a regra padrão, que permite todo o tráfego de saída.
8. Escolha Create security group (Criar grupo de segurança).

Command line

Para criar um security group com o menor privilégio

Use um dos seguintes comandos:

- [create-security-group](#) (AWS CLI)
- [New-EC2SecurityGroup](#) (AWS Tools for Windows PowerShell)

Para obter mais informações, consulte [Grupos de segurança do Amazon EC2 para instâncias do Windows \(p. 1217\)](#).

Tutorial: Comece a usar instâncias Windows do Amazon EC2

Use este tutorial para começar a usar o Amazon Elastic Compute Cloud (Amazon EC2). Você aprenderá a iniciar, conectar-se e usar uma instância Windows. Uma instância é um servidor virtual na Nuvem AWS. Com o Amazon EC2 você pode definir e configurar o sistema operacional e as aplicações que são executadas em sua instância.

Ao se cadastrar na AWS, você poderá começar a usar o Amazon EC2 usando o [Nível gratuito da AWS](#). Se você tiver criado sua conta da AWS há menos de 12 meses e ainda não tiver excedido os benefícios de nível gratuito para o Amazon EC2, você não será cobrado para concluir este tutorial, pois nós o ajudamos a selecionar as opções que estão dentro dos benefícios do nível gratuito. Caso contrário, você incorrerá em taxas de utilização padrão do Amazon EC2 desde o momento em que executar a instância até encerrar a instância (que é a tarefa final deste tutorial), mesmo que ela permaneça ociosa.

Tópicos

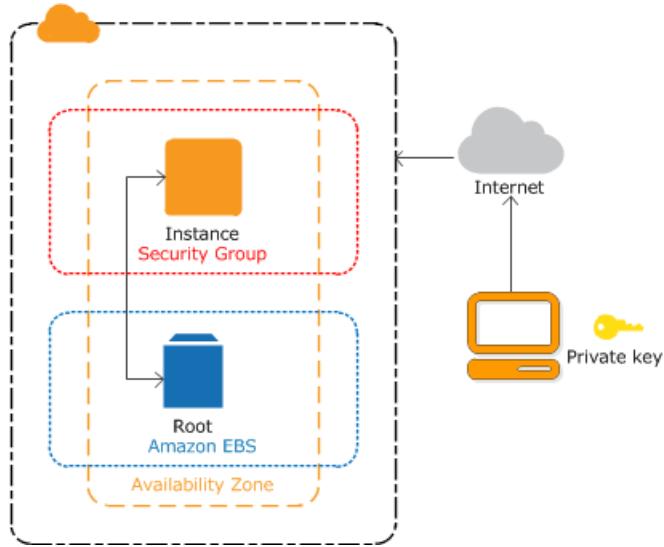
- [Overview \(p. 10\)](#)
- [Prerequisites \(p. 11\)](#)
- [Etapa 1: executar uma instância \(p. 11\)](#)
- [Etapa 2: conectar-se à instância \(p. 12\)](#)
- [Etapa 3: limpar a instância \(p. 18\)](#)
- [Próximas etapas \(p. 18\)](#)

Tutoriais relacionados

- Se você preferir executar uma instância Linux, consulte este tutorial no Guia do usuário do Amazon EC2 para instâncias do Linux: [Conceitos básicos das instâncias Linux do Amazon EC2](#).
- Se você preferir usar a linha de comando, consulte este tutorial no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface): [Using Amazon EC2 through the AWS CLI \(Usar o Amazon EC2 pela AWS CLI\)](#).

Overview

A instância é baseada em Amazon EBS (o que significa que o volume raiz é um volume do EBS). Você pode especificar a zona de disponibilidade na qual sua instância é executada ou deixar o Amazon EC2 selecionar uma zona de disponibilidade para você. Quando você executa a instância, a protege especificando um par de chaves e um security group. Ao se conectar à instância, você deve especificar a chave privada correspondente ao par de chaves especificado ao executar a instância.



Prerequisites

Antes de começar, você deve concluir as etapas em [Configuração para usar o Amazon EC2. \(p. 6\)](#).

Etapa 1: executar uma instância

Você pode executar uma instância Windows utilizando o AWS Management Console como descrito no procedimento a seguir. Este tutorial tem o objetivo de ajudá-lo a executar rapidamente sua primeira instância, então ele não abrange todas as opções possíveis. Para obter mais informações sobre essas opções avançadas, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#). Para obter informações sobre outras formas de executar sua instância, consulte [Executar sua instância \(p. 417\)](#).

Como iniciar uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel do console, selecione Launch Instance.
3. Na página Choose an Amazon Machine Image (AMI), há uma lista de configurações básicas, chamadas Amazon Machine Images (AMIs), que funcionam como modelos para sua instância. Selecione a AMI para o Windows Server 2016 Base ou posterior. Observe que essas AMIs estão marcadas como "Elegíveis para nível gratuito".
4. Na página Choose an Instance Type, você pode selecionar a configuração de hardware de sua instância. Selecione o tipo de instância `t2.micro`, que é selecionado por padrão. O tipo de instância `t2.micro` está qualificado para o nível gratuito. Em regiões onde `t2.micro` não está disponível, você pode usar uma instância `t3.micro` no nível gratuito. Para obter mais informações, consulte [Nível gratuito da AWS](#).
5. Na página Choose an Instance Type (Escolha um tipo de instância), selecione Review and Launch para permitir que o assistente conclua outras definições de configuração para você.
6. Na página Review Instance Launch, em Security Groups, você verá que o assistente criou e selecionou um security group para você. Você pode usar esse security group ou, como opção, pode selecionar o security group que você criou ao realizar a configuração usando as seguintes etapas:

- a. Escolha Edit security groups.
- b. Na página Configure Security Group, garanta que Select an existing security group esteja selecionado.
- c. Selecione o security group na lista de security groups existentes e escolha Review and Launch.
7. Na página Review Instance Launch, escolha Launch.
8. Se um par de chaves for solicitado, selecione Choose an existing key pair e selecione o par de chaves que você criou ao obter a configuração.

Warning

Não selecione Continuar sem um par de chaves. Se você executar sua instância sem um par de chaves, você não poderá conectá-la.

Quando estiver pronto, selecione a caixa de confirmação e, então, escolha Launch Instances.

9. Uma página de confirmação informa que sua instância está sendo executada. Selecione Visualizar instâncias para fechar a página de confirmação e voltar ao console.
10. Na tela Instances, é possível visualizar o status da execução. Demora um pouco para executar uma instância. Ao executar uma instância, seu estado inicial é pending. Após a inicialização da instância, seu estado muda para running e ela recebe um nome DNS público. (Se a coluna Public IPv4 DNS (DNS IPv4 público) estiver oculta, escolha o ícone de configurações () no canto superior direito, alterne o DNS IPv4 público , e clique em Confirm (Confirmar)).
11. Pode levar alguns minutos até que a instância esteja pronta para que você possa se conectar a ela. Verifique se a instância foi aprovada nas verificações de status da coluna Status Checks (Verificações de status).

Etapa 2: conectar-se à instância

Para se conectar a uma instância Windows, você deve recuperar a senha do administrador e inserir essa senha ao se conectar à sua instância usando o desktop remoto. Após a execução da instância, leva alguns minutos para que a senha fique disponível.

O nome da conta de administrador depende do idioma do sistema operacional. Por exemplo, em inglês é Administrator, em francês é Administrateur e em português é Administrador. Para obter mais informações, consulte [Localized Names for Administrator Account in Windows \(Nomes localizados da conta de administrador no Windows\)](#) no Microsoft TechNet Wiki.

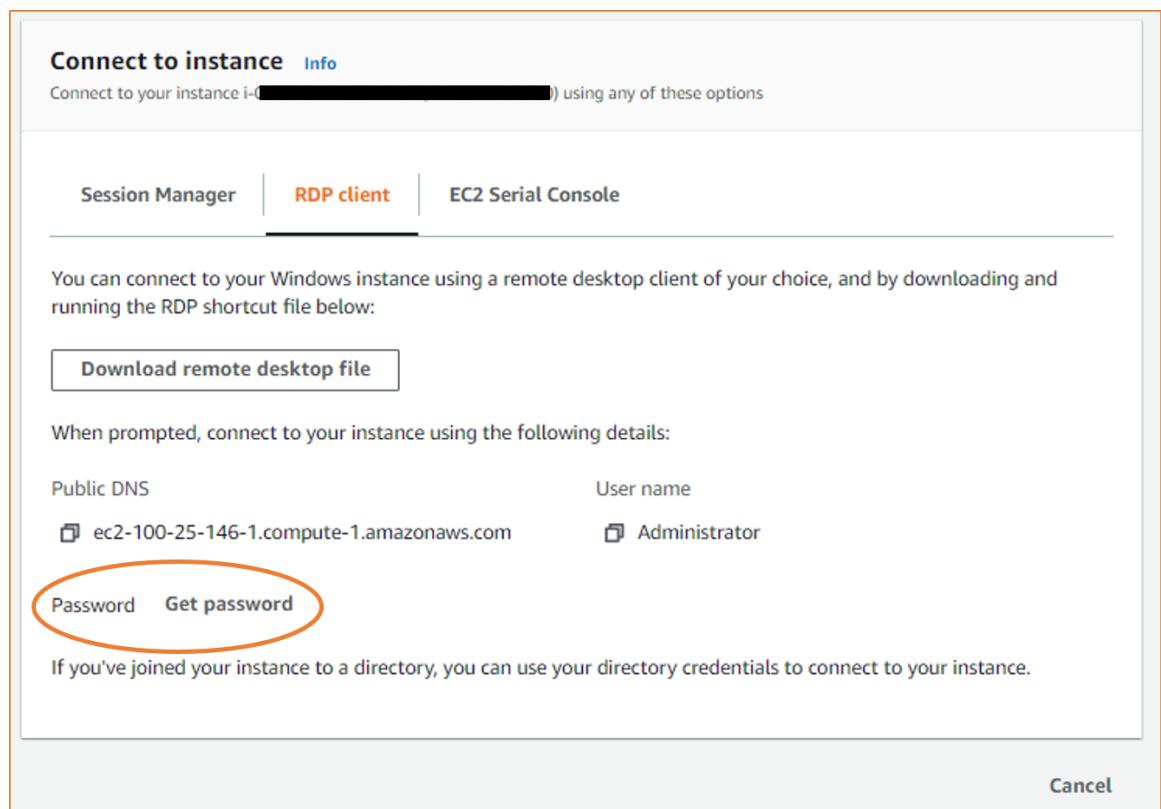
Se você associou sua instância a um domínio, poderá se conectar a sua instância usando credenciais de domínio definidas no AWS Directory Service. Na tela de logon do desktop remoto, em vez de usar o nome do computador local e a senha gerada, use o nome de usuário totalmente qualificado para o administrador (por exemplo, **corp.example.com\Admin**) e a senha dessa conta.

Se você receber um erro ao tentar se conectar à instância, consulte [O Remote Desktop não pode se conectar ao computador remoto \(p. 1574\)](#).

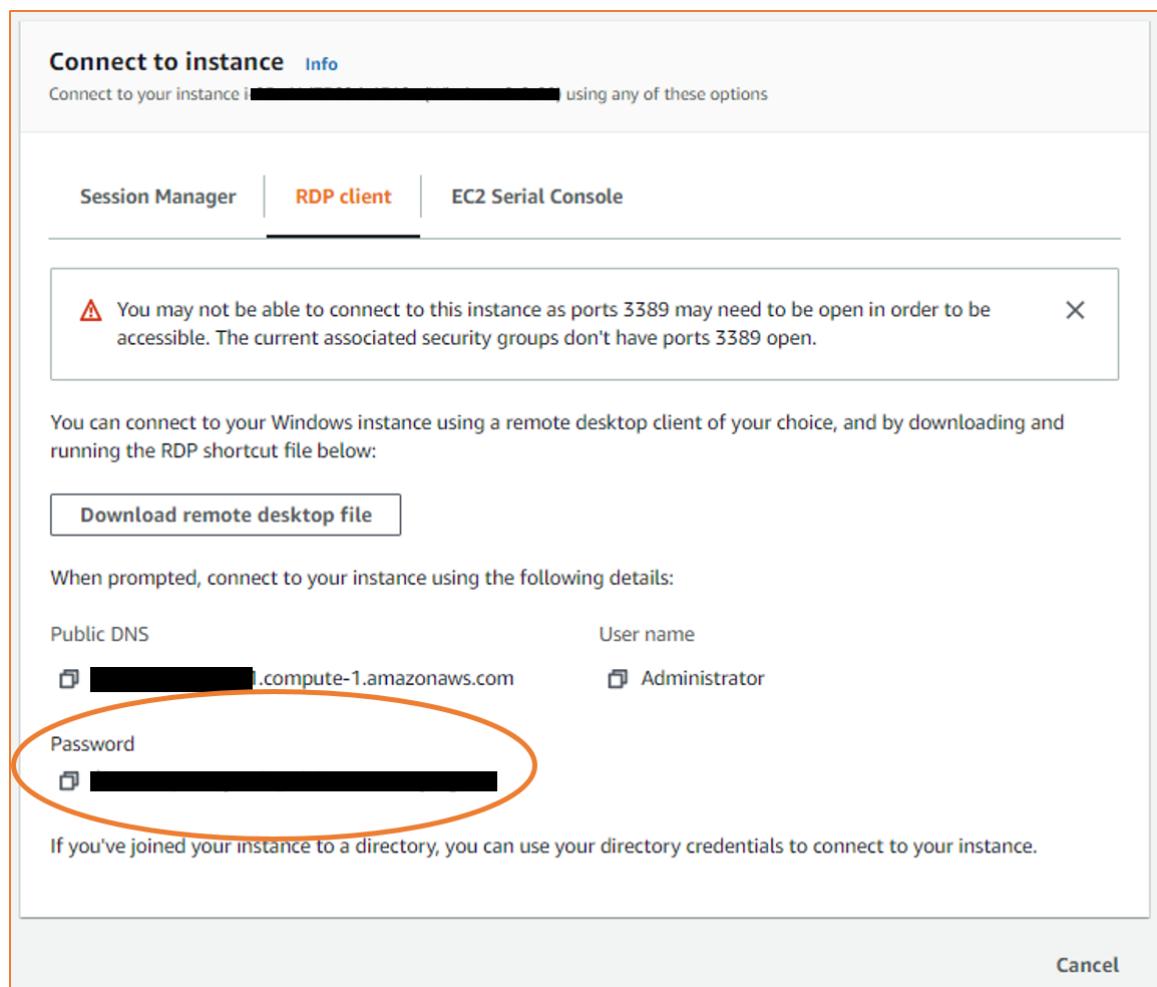
New console

Para se conectar à sua instância do Windows usando um cliente RDP

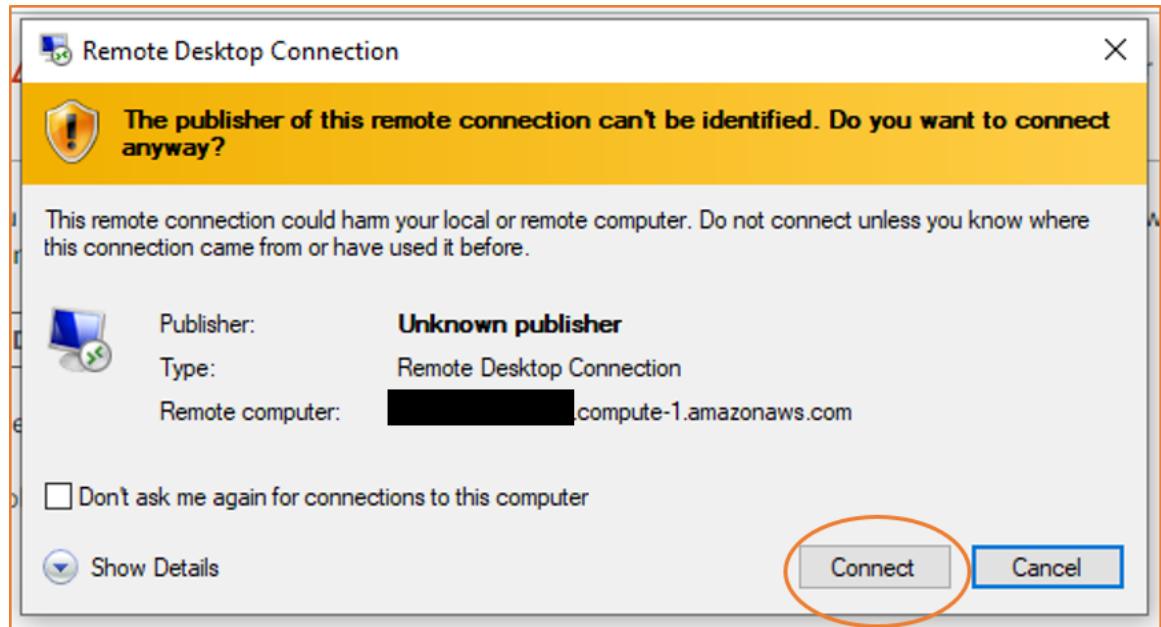
1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instances (Instâncias). Selecione a instância e escolha Conectar.
3. Na página Connect to instance (Conectar à instância), escolha a guia RDP client (Cliente RDP) e depois Get password (Obter senha).



4. Escolha Browse (Navegar) e navegue até o arquivo de chave privada (.pem) que você criou ao iniciar a instância. Selecione o arquivo e escolha Open (Abrir) para copiar todo o conteúdo do arquivo para essa janela.
5. Escolha Decrypt Password. O console exibe a senha de administrador padrão correspondente à instância em Password (Senha), substituindo o link Get Password (Obter senha) exibido anteriormente. Salve a senha em um lugar seguro. Essa senha é necessária para se conectar à instância.



6. Escolha Download remote desktop file (Fazer download de arquivo da área de trabalho remota). O navegador pergunta se você quer abrir ou salvar o arquivo de atalho RDP. Quando terminar o download do arquivo, escolha Cancel (Cancelar) para retornar à página Instances (Instâncias).
 - Se tiver aberto o arquivo RDP, você verá a caixa de diálogo Remote Desktop Connection (Conexão de área de trabalho remota).
 - Se você tiver salvado o arquivo RDP, navegue até o diretório de downloads e abra o arquivo RDP para exibir a caixa de diálogo.
7. Talvez você receba um aviso de que o publicador da conexão remota é desconhecido. Escolha Connect (Conectar) para se conectar à sua instância.

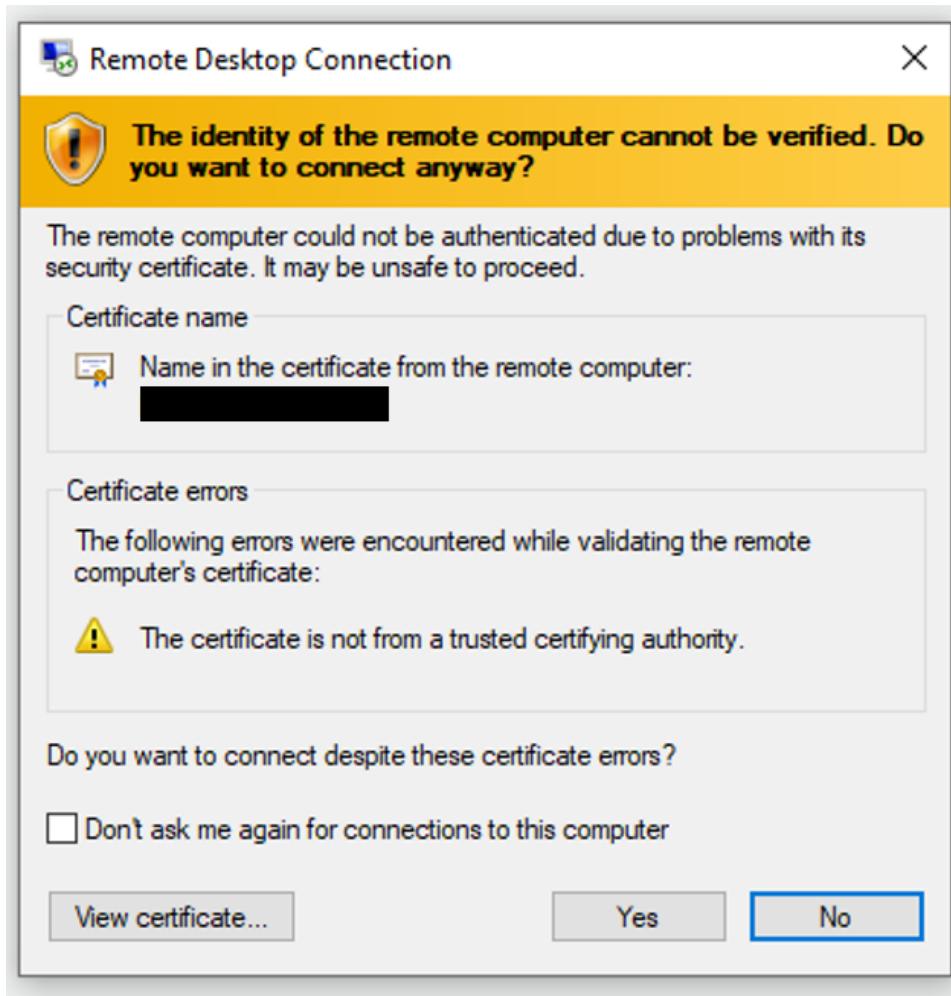


8. A conta de administrador é escolhida por padrão. Copie e cole a senha que você salvou anteriormente.

Tip

Se você receber o erro “Password Failed” (Senha incorreta), tente digitar a senha manualmente. As senhas podem ser corrompidas ao copiar e colar.

9. Devido à natureza dos certificados autoassinados, talvez você receba um aviso indicando que o certificado de segurança não pode ser autenticado. Siga as etapas abaixo para confirmar a identidade do computador remoto ou apenas escolha Yes (Sim) (Windows) ou Continue (Continuar) (Mac OS X) caso confie no certificado.



- a. Se estiver usando a Remote Desktop Connection (Conexão de área de trabalho remota) em um computador Windows, escolha View certificate (Exibir certificado). Se estiver usando o Microsoft Remote Desktop em um Mac, escolha Show Certificate.
- b. Selecione a guia Details (Detalhes) e role para baixo até Thumbprint (Impressão digital) (Windows) ou SHA1 Fingerprints (Impressões digitais SHA1) (Mac OS X). Esse é o identificador exclusivo do certificado de segurança do computador remoto.
- c. No console do Amazon EC2, selecione a instância, escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema).
- d. Procure por RDPCERTIFICATE-THUMBPRINT na saída do log: Se esse valor corresponder à impressão digital do certificado, você terá verificado a identidade do computador remoto.
- e. Se estiver usando a Remote Desktop Connection (Conexão de área de trabalho remota) em um computador Windows, volte à caixa de diálogo Certificate (Certificado) e escolha OK. Se estiver usando o Microsoft Remote Desktop em um Mac, volte para Verify Certificate e escolha Continue.
- f. [Windows] Escolha Yes (Sim) na janela Remote Desktop Connection (Conexão de área de trabalho remota) para se conectar à instância.

[Mac OS X] Faça login conforme solicitado, usando a conta de administrador padrão e a senha de administrador padrão que você registrou ou copiou anteriormente. Observe que pode ser necessário alternar espaços para ver a tela de login. Para obter mais informações, consulte [Add spaces and switch between them](#) (Adicionar espaços e alternar entre eles).

Old console

Para se conectar à sua instância do Windows usando um cliente RDP

1. No console do Amazon EC2, selecione a instância e, em seguida, escolha Connect (Conectar-se).
2. Na caixa de diálogo Connect To Your Instance, escolha Get Password (depois que a instância é lançada, demora alguns minutos para que a senha fique disponível).
3. Escolha Browse (Navegar) e navegue até o arquivo de chave privada (.pem) que você criou ao iniciar a instância. Selecione o arquivo e escolha Open para copiar todo o conteúdo do arquivo para o campo Contents.
4. Escolha Decrypt Password. O console exibe a senha de administrador padrão correspondente à instância na caixa de diálogo Connect To Your Instance, substituindo o link para Get Password mostrado anteriormente pela senha real.
5. Registre a senha de administrador padrão ou copie-para a área de transferência. Você precisará dessa senha para se conectar à instância.
6. Escolha Download Remote Desktop File. O navegador pergunta se você quer abrir ou salvar o arquivo .rdp. Qualquer uma das opções é aceitável. Quando terminar, você poderá escolher Close para descartar a caixa de diálogo Connect To Your Instance.
 - Se tiver aberto o arquivo .rdp, você verá a caixa de diálogo Remote Desktop Connection (Conexão da área de trabalho remota).
 - Se você tiver salvado o arquivo .rdp, navegue até o diretório de downloads e abra o arquivo .rdp para exibir a caixa de diálogo.
7. Talvez você receba um aviso de que o publicador da conexão remota é desconhecido. Você pode continuar se conectando à instância.
8. Quando solicitado, faça login na instância usando a conta do administrador do sistema operacional e a senha registrada ou copiada por você anteriormente. Caso sua Remote Desktop Connection (Conexão da área de trabalho remota) já tenha uma conta de administrador configurada, talvez seja necessário escolher a opção Use another account (Usar outra conta) e digitar o nome de usuário e senha manualmente.

Note

Às vezes, quando se copia e cola conteúdo, os dados podem ser corrompidos. Se você encontrar o erro "Password Failed" ao fazer login, experimente digitar a senha manualmente.

9. Devido à natureza dos certificados autoassinados, talvez você receba um aviso indicando que o certificado de segurança não pôde ser autenticado. Siga as etapas abaixo para confirmar a identidade do computador remoto ou apenas escolha Yes ou Continue para continuar, caso confie no certificado.
 - a. Se estiver usando a Conexão de área de trabalho remota em um PC Windows, escolha View certificate. Se estiver usando o Microsoft Remote Desktop em um Mac, escolha Show Certificate.
 - b. Escolha a guia Details (Detalhes) e role a tela para baixo até a entrada Thumbprint (Impressão digital) em um PC com o Windows ou a entrada SHA1 Fingerprints (Impressões digitais com SHA1) em um Mac. Esse é o identificador exclusivo do certificado de segurança do computador remoto.
 - c. No console do Amazon EC2, selecione a instância, escolha Actions (Ações) e, em seguida, escolha Get System Log (Obter log do sistema).
 - d. Na saída do log do sistema, procure uma entrada rotulada RDPCERTIFICATE-THUMBPRINT. Se esse valor corresponder à impressão digital do certificado, você terá verificado a identidade do computador remoto.

- e. Se estiver usando a Conexão de área de trabalho remota em um PC Windows, volte à caixa de diálogo Certificate e escolha OK. Se estiver usando o Microsoft Remote Desktop em um Mac, volte para Verify Certificate e escolha Continue.
- f. [Windows] Escolha Yes na janela Remote Desktop Connection para se conectar à instância.
[Mac OS] Faça login conforme solicitado, usando a conta de administrador padrão e a senha de administrador padrão que você registrou ou copiou anteriormente. Observe que pode ser necessário alternar espaços para ver a tela de login. Para mais informações sobre espaços, consulte [support.apple.com/pt-br/HT204100](#).
- g. Se você receber um erro ao tentar se conectar à instância, consulte [O Remote Desktop não pode se conectar ao computador remoto \(p. 1574\)](#).

Etapa 3: limpar a instância

Após concluir a instância que você criou para este tutorial, você deverá limpar encerrando a instância. Se você quiser realizar outras ações com essa instância antes de limpá-la, consulte [Próximas etapas \(p. 18\)](#).

Important

Encerrar uma instância significa excluí-la efetivamente, pois você não poderá mais reconectá-la depois dessa ação.

Se você estiver executando uma instância que não está no [Nível gratuito da AWS](#), você deixará de ser cobrado por essa instância assim que o status da instância for alterado para `shutting down` ou `terminated`. Para manter sua instância para depois, sem a cobrança de taxas, você poderá interromper a instância agora e iniciá-la novamente mais tarde. Para obter mais informações, consulte [Interromper e iniciar sua instância \(p. 455\)](#).

Para encerrar sua instância

1. No painel de navegação, escolha Instances (Instâncias). Na lista de instâncias, selecione a instância.
2. Escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).
3. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

O Amazon EC2 desliga e encerra sua instância. Depois que a instância for encerrada, ela permanecerá visível no console por um curto período e a entrada será automaticamente excluída. Você não pode remover a instância encerrada da exibição do console.

Próximas etapas

Após iniciar sua instância, talvez você queira tentar alguns dos seguintes exercícios:

- Saiba como gerenciar remotamente a instância do EC2 utilizando Executar comando. Para obter mais informações, consulte [AWS Systems Manager Run Command](#) (Run Command do AWS Systems Manager) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).
- Configure um alarme do CloudWatch para notificá-lo caso seu uso ultrapasse o Nível gratuito. Para obter mais informações, consulte [Tracking your AWS Free Tier usage](#) (Monitorar o uso do nível gratuito da AWS) no AWS Billing and Cost Management User Guide (Manual do usuário do AWS Billing and Cost Management).
- Adicione um volume do EBS. Para obter mais informações, consulte [Crie um volume do Amazon EBS. \(p. 1268\)](#) e [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#).

Melhores práticas do Windows no Amazon EC2

Esta lista de práticas ajudará você a obter os melhores resultados da execução do Windows no Amazon EC2.

Atualizar drivers do Windows

Mantenha os drivers mais recentes em todas as instâncias do EC2 do Windows para garantir que as correções de problemas e melhorias de desempenho mais recentes sejam aplicadas em toda a sua frota. Dependendo do tipo de instância, você deve atualizar os drivers PV, ENA e NVMe da AWS.

- Utilize o [Trusted Advisor](#) para manter o Windows do Amazon EC2 atualizado com os drivers do Windows fornecidos pela AWS.
- Use [tópicos do SNS](#) para receber atualizações de novos lançamentos de driver.
- Use o documento [AWSSupport-UpgradeWindowsAWSDrivers](#) do SSM do AWS Systems Manager para aplicar facilmente as atualizações em todas as instâncias.

Executar novas instâncias com as AMIs mais recentes do Windows

A AWS lança novas [AMIs do Windows](#) a cada mês, o que contém os drivers, agentes de execução e patches do SO mais recentes. Você deve utilizar a AMI mais recente ao executar novas instâncias ou ao criar suas próprias imagens personalizadas.

- Para criar com as AMIs mais recentes disponíveis, consulte [Consulta para a AMI mais recente do Windows usando o Systems Manager Parameter Store](#).

Testar o desempenho do sistema/aplicativo antes da mitigação

Migrar aplicativos empresariais para a AWS pode envolver muitas variáveis e configurações. Sempre teste o desempenho da solução do EC2 para garantir que:

- Os tipos de instância estão configurados corretamente, incluindo o tamanho da instância, as redes avançadas e a locação (compartilhada ou dedicada).
- A topologia da instância é adequada para a carga de trabalho e utiliza recursos de alto desempenho quando necessário (locação dedicada, grupos de alocação, volumes de armazenamento de instâncias, bare metal).

Atualizar agentes de execução

Atualize para o agente EC2Launch v2 (Windows Server 2008 e posterior) mais recente para garantir que as correções de problemas mais recentes sejam aplicadas em toda a sua frota. Para atualizar, consulte as instruções em [Instale a versão mais recente do EC2Launch v2](#).

Se você quiser continuar usando os agentes EC2Config (Windows Server 2012 R2 e anteriores) ou EC2Launch (Windows Server 2016 e posteriores), certifique-se de que as correções de problemas mais recentes sejam aplicadas em toda a frota.

- Para obter instruções de atualização do EC2Config, consulte [Instalar a versão mais recente do EC2Config](#).

- Para obter instruções de atualização do EC2Launch, consulte [Instalar a versão mais recente do EC2Launch](#).

Security

Ao proteger instâncias do Windows, recomendamos que você implemente os Serviços de Domínio do Active Directory para habilitar uma infraestrutura escalável, segura e gerenciável para locais distribuídos. Além disso, depois de executar instâncias por meio do Console AWS ou usar uma ferramenta de provisionamento do Amazon EC2, como AWS CloudFormation, é recomendável utilizar recursos nativos do SO, como o [Microsoft Windows PowerShell DSC](#), para manter o estado de configuração em caso de oscilação de configuração.

As instâncias do Windows na AWS devem aderir às seguintes práticas recomendadas de alto nível:

- Acesso mínimo: conceda acesso somente a sistemas e locais confiáveis e esperados. Isso se aplica a todos os produtos da Microsoft, como o Active Directory, servidores de produtividade empresarial da Microsoft e serviços de infraestrutura, como Serviços de área de trabalho remota, servidores de proxy reverso, servidores Web IIS etc. Use os recursos da AWS, como os grupos de segurança da instância do Amazon EC2, listas de controle de acesso (ACLs) à rede e sub-redes públicas/privadas da Amazon VPC, para colocar a segurança em camadas em vários locais em uma arquitetura. Em uma instância do Windows, os clientes podem usar o Firewall do Windows para colocar mais uma camada na estratégia de defesa completa em sua implantação. Instale apenas os componentes e aplicativos do sistema operacional necessários para que o sistema funcione conforme projetado. Configure serviços de infraestrutura, como o IIS, para serem executados em contas de serviço ou para usar recursos como identidades de grupo de aplicativos para acessar recursos local e remotamente na infraestrutura.
- Menos privilégio: determine o conjunto mínimo de privilégios de que as instâncias e contas precisam para executar suas funções. Restringir esses servidores e usuários para permitir apenas essas permissões definidas. Use técnicas, como controles de acesso baseados em função, para reduzir a área de superfície das contas administrativas e criar as funções mais limitadas para realizar uma tarefa. Use recursos do sistema operacional, como o Encrypting File System (EFS – Criptografia do sistema de arquivos) dentro do NTFS, para criptografar dados confidenciais em repouso e controlar o acesso de aplicativo e de usuário a ele.
- Gerenciamento de configuração: crie uma configuração de servidor de linha de base que incorpore patches de segurança atualizados e conjuntos de proteção baseados em host que incluem antivírus, antimalware, detecção/prevenção de invasões e monitoramento de integridade de arquivos. Avalie cada servidor em relação à linha de base registrada atual para identificar e sinalizar quaisquer desvios. Verifique se cada servidor está configurado para gerar e armazenar com segurança os dados adequados de log e auditoria. Para obter mais informações sobre como atualizar a instância Windows, consulte [Como atualizar a instância do Windows](#).
- Gerenciamento de alterações: crie processos para controlar alterações nas linhas de base da configuração do servidor e trabalhe em processos de alteração totalmente automatizados. Além disso, aproveite Just Enough Administration (JEA) com o Windows PowerShell DSC para limitar o acesso administrativo às funções mínimas necessárias.
- Logs de auditoria: audite o acesso e todas as alterações nas instâncias do Amazon EC2 para verificar a integridade do servidor e garantir que apenas as alterações autorizadas sejam feitas. Utilize funcionalidades como [Enhanced Log for IIS \(Log aprimorado para IIS\)](#) para melhorar os recursos de registo de log padrão. Os recursos da AWS como Logs de fluxo da VPC e AWS CloudTrail também estão disponíveis para auditar o acesso à rede, incluindo solicitações permitidas/negadas e chamadas de API, respectivamente.

Storage

- Use volumes do Amazon EBS separados para o sistema operacional e para seus dados. Verifique se o volume com seus dados persiste depois do encerramento de uma instância. Para obter mais informações, consulte [Preservar volumes do Amazon EBS no encerramento da instância \(p. 478\)](#).

- Use o armazenamento de instâncias disponível para que sua instância armazene dados temporários. Lembre-se de que os dados armazenados em um armazenamento de instâncias são excluídos quando você interrompe, hiberna ou encerra uma instância. Se você usar o armazenamento de instâncias para armazenamento de bancos de dados, verifique se você tem um cluster com um fator de replicação que garanta tolerância a falhas.
- Criptografe volumes e snapshots do EBS. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).

Gerenciamento de recursos

- Use os metadados da instância e as tags personalizadas dos recursos para acompanhar e identificar os recursos da AWS. Para obter mais informações, consulte [Metadados da instância e dados do usuário \(p. 622\)](#) e [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).
- Visualize seus limites atuais para o Amazon EC2. Planeje a solicitação de aumentos dos limites com antecedência antes que sejam necessários. Para obter mais informações, consulte [Cotas de serviço do Amazon EC2 \(p. 1567\)](#).

Backup e recuperação

- Faça backup de seus volumes do EBS regularmente usando [Snapshots do Amazon EBS \(p. 1294\)](#) e crie uma [Imagen de máquina da Amazon \(AMI\) \(p. 22\)](#) de sua instância para salvar a configuração como um modelo para executar futuras instâncias.
- Implante os componentes essenciais de seu aplicativo em várias zonas de disponibilidade e replique os dados adequadamente.
- Crie seus aplicativos para lidarem com o endereçamento IP dinâmico quando sua instância for reiniciada. Para obter mais informações, consulte [Endereçamento IP de instâncias do Amazon EC2 \(p. 956\)](#).
- Monitorar e responder a eventos. Para obter mais informações, consulte [Monitorar o Amazon EC2 \(p. 864\)](#).
- Certifique-se de que você está preparado para lidar com failover. Para uma solução básica, você pode anexar manualmente uma interface de rede ou um endereço IP elástico para uma instância de substituição. Para obter mais informações, consulte [Interfaces de rede elástica \(p. 1002\)](#). Para uma solução automatizada, você pode usar o Amazon EC2 Auto Scaling. Para mais informações, consulte o [Guia do usuário do Amazon EC2 Auto Scaling](#).
- Teste regularmente o processo de recuperação de suas instâncias e de volumes do Amazon EBS em caso de falha.

Networking

- Defina a vida útil (TTL) de seus aplicativos como 255, para IPv4 e IPv6. Se você usar um valor menor, a TTL poderá expirar enquanto o tráfego do aplicativo estiver em trânsito, causando problemas de acessibilidade para as instâncias.

Imagens de máquina da Amazon (AMIs)

Uma Imagem de máquina da Amazon (AMI) fornece as informações necessárias para iniciar uma instância. Você deve especificar uma AMI ao iniciar uma instância. Você pode executar várias instâncias em uma única AMI quando precisa de várias instâncias com a mesma configuração. Você pode usar AMIs diferentes para executar instâncias quando precisa de instâncias com configurações diferentes.

Uma AMI inclui o seguinte:

- Um ou mais snapshots do Amazon Elastic Block Store (Amazon EBS) ou, para AMIs com suporte de armazenamento de instâncias, um modelo para o volume raiz da instância (por exemplo, um sistema operacional, um servidor da aplicação e aplicações).
- Permissões de execução que controlam quais contas da AWS podem usar a AMI para executar instâncias.
- Um mapeamento de dispositivos de blocos que especifica os volumes a serem anexados à instância quando ela for executada.

Tópicos

- [Modos de inicialização \(p. 22\)](#)
- [AWSAMIs do Windows \(p. 29\)](#)
- [Localizar uma AMI do Windows \(p. 102\)](#)
- [AMIs compartilhadas \(p. 108\)](#)
- [AMIs pagas \(p. 115\)](#)
- [Ciclo de vida da AMI \(p. 120\)](#)
- [Usar criptografia com AMIs com EBS \(p. 135\)](#)
- [Noções básicas sobre as informações de faturamento da AMI \(p. 140\)](#)

Modos de inicialização

Quando um computador é inicializado, o primeiro software executado é responsável por inicializar a plataforma e fornecer uma interface para que o sistema operacional execute operações específicas da plataforma.

Modos de inicialização padrão

No EC2, duas variantes do software do modo de inicialização são suportadas: BIOS legado e Unified Extensible Firmware Interface (UEFI). Por padrão, os tipos de instância Intel e AMD são executados em BIOS legado e os tipos de instância Graviton são executados em UEFI.

Como executar tipos de instâncias Intel e AMD em UEFI

[Most Intel and AMD instance types](#) pode ser executado em UEFI e BIOS herdado. Para usar UEFI, é preciso selecionar uma AMI com o parâmetro de modo de inicialização definido como uefi, e o sistema operacional contido na AMI deve ser configurado para suportar UEFI.

Objetivo do parâmetro de modo de inicialização da AMI

O parâmetro de modo de inicialização da AMI sinaliza ao EC2 qual modo de inicialização usar ao iniciar uma instância. Quando o parâmetro de modo de inicialização é definido como uefi, o EC2 tenta iniciar a instância em UEFI. Se o sistema operacional não estiver configurado para oferecer suporte a UEFI, a execução da instância poderá falhar.

Warning

Definir o parâmetro de modo de inicialização não configura automaticamente o sistema operacional para o modo de inicialização especificado. A configuração é específica para o sistema operacional. Para obter as instruções de configuração, consulte o manual do sistema operacional.

Possível parâmetro de modo de inicialização em uma AMI

O parâmetro de modo de inicialização da AMI é opcional. Uma AMI pode ter um dos seguintes valores de parâmetro de modo de inicialização: uefi ou legacy-bios. Algumas AMIs não têm um parâmetro de modo de inicialização. Para AMIs sem parâmetro de modo de inicialização, as instâncias executadas a partir delas usam o valor padrão do tipo de instância—uefi no Graviton e legacy-bios em todos os tipos de instância Intel e AMD.

Tópicos

- [Considerations \(p. 23\)](#)
- [Requisitos para executar uma instância com UEFI \(p. 23\)](#)
- [Determinar o parâmetro de modo de inicialização de uma AMI \(p. 24\)](#)
- [Determinar os modos de inicialização suportados por um tipo de instância \(p. 25\)](#)
- [Determinar o modo de inicialização de uma instância \(p. 25\)](#)
- [Determinar o modo de inicialização do sistema operacional \(p. 26\)](#)
- [Definir o modo de inicialização de uma AMI \(p. 26\)](#)

Considerations

- Modos de inicialização padrão:
 - Tipos de instância Intel e AMD: BIOS legado
 - Tipos de instância Graviton: UEFI
- Os tipos de instância Intel e AMD compatíveis com UEFI, além de BIOS herdado:
 - Virtualizado: C5, C5a, C5ad, C5d, C5n, D3, D3en, G4, I3en, M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, R5, R5a, R5ad, R5b, R5d, R5dn, R5n, T3, T3a e z1d
- No momento, o UEFI Secure Boot não é suportado.

Requisitos para executar uma instância com UEFI

Para executar uma instância no modo UEFI, é preciso selecionar um tipo de instância compatível com UEFI e configurar a AMI e o sistema operacional para UEFI, da seguinte forma:

- Tipo de instância – Ao executar uma instância, é preciso selecionar um tipo de instância compatível com UEFI. Para obter mais informações, consulte [Determinar os modos de inicialização suportados por um tipo de instância \(p. 25\)](#).
- AMI – Ao executar uma instância, é preciso selecionar uma AMI configurada para UEFI. A AMI deve ser configurada da seguinte forma:
 - SO – O sistema operacional contido na AMI deve ser configurado para usar UEFI; caso contrário, a execução da instância falhará. Para obter mais informações, consulte [Determinar o modo de inicialização do sistema operacional \(p. 26\)](#).

-
- Parâmetro de modo de inicialização da AMI – O parâmetro de modo de inicialização da AMI deve ser definido como `uefi`. Para obter mais informações, consulte [Determinar o parâmetro de modo de inicialização de uma AMI \(p. 24\)](#).

A AWS não fornece AMIs previamente configuradas para oferecer suporte a UEFI. É necessário [configurar a AMI \(p. 26\)](#), importe a AMI através do [VM Import/Export](#), ou importe a AMI através do [CloudEndure](#).

Determinar o parâmetro de modo de inicialização de uma AMI

O parâmetro de modo de inicialização da AMI é opcional. Uma AMI pode ter um dos seguintes valores de parâmetro de modo de inicialização: `uefi` e `legacy-bios`.

Algumas AMIs não têm um parâmetro de modo de inicialização. Quando uma AMI não tem parâmetro de modo de inicialização, as instâncias executadas a partir dela usam o valor padrão do tipo de instância, que é `uefi` no Graviton e `legacy-bios` nos tipos de instância Intel e AMD.

Para determinar o parâmetro de modo de inicialização de uma AMI (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha AMIs e, em seguida, selecione a AMI.
3. Na guia Details (Detalhes), verifique o campo Boot mode (Modo de inicialização).

Para determinar o parâmetro de modo de inicialização de uma AMI ao executar uma instância (console)

Ao executar uma instância usando o assistente de instância de execução, na etapa de selecionar uma AMI, verifique o campo Boot mode (Modo de inicialização). Para obter mais informações, consulte [Etapa 1: Escolher uma imagem de máquina da Amazon \(AMI\) \(p. 419\)](#).

Para determinar o parâmetro do modo de inicialização de uma AMI (AWS CLI versão 1.19.34 e posterior e versão 2.1.32 e posterior)

Use o comando `describe-images` para determinar o modo de inicialização de uma AMI.

```
aws ec2 --region us-east-1 describe-images --image-id ami-0abcdef1234567890
```

Saída esperada

```
{
  "Images": [
    {
      ...
    },
    {
      "EnaSupport": true,
      "Hypervisor": "xen",
      "ImageOwnerAlias": "amazon",
      "Name": "UEFI_Boot_Mode_Enabled-Windows_Server-2016-English-Full-Base-2020.09.30",
      "RootDeviceName": "/dev/sda1",
      "RootDeviceType": "ebs",
      "SriovNetSupport": "simple",
      "VirtualizationType": "hvm",
      "BootMode": "uefi"
    }
  ]
}
```

Determinar os modos de inicialização suportados por um tipo de instância

Para determinar os modos de inicialização compatíveis de um tipo de instância (AWS CLI versão 1.19.34 e posterior e versão 2.1.32 e posterior)

Use o comando [describe-instance-types](#) para determinar os modos de inicialização suportados por um tipo de instância. A incluir o parâmetro --query, você pode filtrar a saída. Neste exemplo, a saída é filtrada para retornar somente os modos de inicialização suportados.

O exemplo a seguir mostra que m5.2xlarge suporta ambos os modos de inicialização UEFI e BIOS legado.

```
aws ec2 --region us-east-1 describe-instance-types --instance-types m5.2xlarge --query "InstanceTypes[*].SupportedBootModes"
```

Saída esperada

```
[  
  [  
    "legacy-bios",  
    "uefi"  
  ]  
]
```

O exemplo a seguir mostra que t2.xlarge suporta apenas BIOS legado.

```
aws ec2 --region us-east-1 describe-instance-types --instance-types t2.xlarge --query "InstanceTypes[*].SupportedBootModes"
```

Saída esperada

```
[  
  [  
    "legacy-bios"  
  ]  
]
```

Determinar o modo de inicialização de uma instância

Quando uma instância é iniciada, o valor do parâmetro de modo de inicialização é determinado pelo valor do parâmetro de modo de inicialização da AMI usado para iniciá-la, da seguinte maneira:

- Uma AMI com um parâmetro de modo de inicialização uefi cria uma instância com um parâmetro de modo de inicialização uefi.
- Uma AMI com um parâmetro de modo de inicialização legacy-bios cria uma instância sem parâmetro de modo de inicialização. Uma instância sem parâmetro de modo de inicialização usa seu valor padrão, que neste caso é legacy-bios.
- Uma AMI sem valor de parâmetro de modo de inicialização cria uma instância sem valor de parâmetro de modo de inicialização.

O valor do parâmetro de modo de inicialização da instância determina o modo em que ela inicializa. Se não houver valor, o modo de inicialização padrão será usado, que é uefi no Graviton e legacy-bios nos tipos de instância Intel e AMD.

Para determinar o modo de inicialização de uma instância (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. Na guia Details (Detalhes), verifique o campo Boot mode (Modo de inicialização).

Para determinar o modo de inicialização de uma instância (AWS CLI versão 1.19.34 e posterior e versão 2.1.32 e posterior)

Use o comando [describe-instances](#) para determinar o modo de inicialização de uma instância.

```
aws ec2 --region us-east-1 describe-instances --instance-ids i-1234567890abcdef0
```

Saída esperada

```
{  
    "Reservations": [  
        {  
            "Groups": [],  
            "Instances": [  
                {  
                    "AmiLaunchIndex": 0,  
                    "ImageId": "ami-0e2063e7f6dc3bee8",  
                    "InstanceId": "i-1234567890abcdef0",  
                    "InstanceType": "m5.2xlarge",  
                    ...  
                },  
                {  
                    "BootMode": "uefi"  
                }  
            ],  
            "OwnerId": "1234567890",  
            "ReservationId": "r-1234567890abcdef0"  
        }  
    ]  
}
```

Determinar o modo de inicialização do sistema operacional

O modo de inicialização do sistema operacional orienta o EC2 sobre o modo de inicialização que deve ser usado para inicializar uma instância. Para verificar se o sistema operacional da instância está configurado para UEFI, é preciso se conectar à instância via RDP.

Para determinar o modo de inicialização do sistema operacional da instância

1. [Conecte-se à instância do Windows usando RDP \(p. 443\).](#)
2. Acesse System Information (Informações do sistema) e verifique a linha BIOS Mode (Modo BIOS).

Definir o modo de inicialização de uma AMI

Ao criar uma AMI usando o comando [register-image](#), é possível definir o modo de inicialização da AMI como uefi ou legacy-bios.

Para converter uma instância existente baseada em BIOS legado para UEFI, ou uma instância existente baseada em UEFI para BIOS legado, é preciso executar uma série de etapas: primeiro, modifique o volume e o sistema operacional da instância para suportar o modo de inicialização selecionado. Em seguida, crie um snapshot do volume. Por fim, use [register-image](#) para criar a AMI usando o snapshot.

Não é possível definir o modo de inicialização de uma AMI usando o comando [create-image](#). Com [create-image](#), a AMI herda o modo de inicialização da instância do EC2 usada para criar a AMI. Por exemplo, se você criar uma AMI a partir de uma instância do EC2 executando em BIOS legado, o modo de inicialização da AMI será configurado como `legacy-bios`.

Warning

Antes de prosseguir com essas etapas, é preciso fazer modificações adequadas no volume e no sistema operacional da instância para oferecer suporte à inicialização através do modo de inicialização selecionado; caso contrário, a AMI resultante não será utilizável. Por exemplo, se você estiver convertendo uma instância baseada em BIOS herdado para UEFI, é possível usar a ferramenta [MBR2GPT](#) da Microsoft para converter o disco do sistema de MBR para GPT. As modificações necessárias são específicas do sistema operacional. Para obter mais informações, consulte o manual do sistema operacional.

Para definir o modo de inicialização de uma AMI (AWS CLI versão 1.19.34 e posterior e versão 2.1.32 e posterior)

1. Faça as modificações adequadas no volume e no sistema operacional da instância para suportar a inicialização através do modo de inicialização selecionado. As modificações necessárias são específicas do sistema operacional. Para obter mais informações, consulte o manual do sistema operacional.

Note

Se você não executar esta etapa, a AMI não será utilizável.

2. Para localizar o ID do volume da instância, use o comando [describe-instances](#). Você criará um snapshot desse volume na próxima etapa.

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0
```

Saída esperada

```
...
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "AttachTime": "",
                "DeleteOnTermination": true,
                "Status": "attached",
                "VolumeId": "vol-1234567890abcdef0"
            }
        }
    ...
}
```

3. Para criar um snapshot do volume, use o comando [create-snapshot](#). Use o ID do volume da etapa anterior.

```
aws ec2 create-snapshot --region us-east-1 --volume-id vol-1234567890abcdef0
--description "add text"
```

Saída esperada

```
{  
    "Description": "add text",  
    "Encrypted": false,  
    "OwnerId": "123",  
    "Progress": "",  
    "SnapshotId": "snap-01234567890abcdef",  
    "StartTime": "",  
    "State": "pending",  
    "VolumeId": "vol-1234567890abcdef0",  
    "VolumeSize": 30,  
    "Tags": []  
}
```

4. Guarde o ID do snapshot na saída da etapa anterior.
5. Aguarde até que a criação do snapshot seja completed antes de ir para a próxima etapa. Para consultar o estado do snapshot, use o comando [describe-snapshots](#).

```
aws ec2 describe-snapshots --region us-east-1 --snapshot-ids snap-01234567890abcdef
```

Exemplo de saída

```
{  
    "Snapshots": [  
        {  
            "Description": "This is my snapshot",  
            "Encrypted": false,  

```

6. Para criar uma nova AMI, use o comando [register-image](#). Use o ID de snapshot que você guardou na etapa anterior. Para definir o modo de inicialização como UEFI, adicione o parâmetro --boot-mode uefi ao comando.

```
aws ec2 register-image \  
    --region us-east-1 \  
    --description "add description" \  
    --name "add name" \  
    --block-device-mappings "DeviceName=/dev/  
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \  
    --architecture x86_64 \  
    --root-device-name /dev/sda1 \  
    --virtualization-type hvm \  
    --ena-support \  
    --boot-mode uefi
```

Saída esperada

```
{  
    "ImageId": "ami-new_ami_123"  
}
```

7. Para verificar se a AMI recém-criada tem o modo de inicialização especificado na etapa anterior, use o comando [describe-images](#).

```
aws ec2 describe-images --region us-east-1 --image-id ami-new_ami_123
```

Saída esperada

```
{  
    "Images": [  
        {  
            "Architecture": "x86_64",  
            "CreationDate": "2021-01-06T14:31:04.000Z",  
            "ImageId": "ami-new_ami_123",  
            "ImageLocation": "",  
            ...  
            "BootMode": "uefi"  
        }  
    ]  
}
```

8. Execute uma nova instância usando a AMI recém-criada. Todas as novas instâncias criadas a partir desta AMI herdarão o mesmo modo de inicialização.
9. Para verificar se a nova instância tem o modo de inicialização esperado, use o comando [describe-instances](#).

AWSAMIs do Windows

AWSA oferece um conjunto de AMIs publicamente disponíveis que contêm configurações de software específicas à plataforma Windows. Usando essas AMIs, você pode começar a criar e a implantar suas aplicações rapidamente usando o Amazon EC2. Primeiro, escolha a AMI que atende a seus requisitos específicos e execute uma instância usando essa AMI. Você recupera a senha da conta do administrador e faz login na instância usando a Conexão de Desktop Remoto, exatamente da mesma forma como com qualquer outro servidor do Windows.

Ao iniciar uma instância de uma AMI do Windows, o dispositivo raiz da instância do Windows é um volume do Amazon Elastic Block Store (Amazon EBS). As AMIs do Windows não são compatíveis com o armazenamento de instâncias no dispositivo raiz.

Entre algumas dessas AMIs do Windows está uma edição do Microsoft SQL Server (SQL Enterprise Edition, SQL Server Standard, SQL Server Express ou SQL Server Web). Executar uma instância em uma AMI do Windows com o Microsoft SQL Server permite executar a instância como um servidor de banco de dados. Como alternativa, você pode executar uma instância em qualquer AMI do Windows e instalar o software de banco de dados necessário na instância.

A Microsoft não oferece mais suporte ao Windows Server 2003, 2008 e 2008 R2. Recomendamos que você execute novas instâncias do EC2 usando uma versão suportada do Windows Server. Se você tiver instâncias do EC2 existentes nas quais haja uma versão incompatível do Windows Server em execução, recomendamos atualizar essas instâncias para uma versão compatível do Windows Server. Para obter mais informações, consulte [Atualizar uma instância do Amazon EC2 do Windows para uma versão mais recente do Windows Server. \(p. 676\)](#).

Tópicos da AMI do Windows

- [Selecionar uma AMI inicial do Windows \(p. 30\)](#)
- [Manter suas AMIs atualizadas \(p. 30\)](#)
- [Tipos de virtualização \(p. 30\)](#)
- [AMIs do Windows gerenciadas pela AWS \(p. 30\)](#)
- [Criar uma AMI do Windows personalizada \(p. 39\)](#)

- [Cancelar o registro da AMI do Windows \(p. 55\)](#)
- [AMIs especializadas do Windows \(p. 56\)](#)
- [AWSHistórico de versões da AMI do Windows da \(p. 62\)](#)

Selecionar uma AMI inicial do Windows

Para visualizar as AMIs do Windows fornecidas pela AWS, você pode usar o console do Amazon EC2 ou o [AWS Marketplace](#). Para obter mais informações, consulte [Localizar uma AMI do Windows \(p. 102\)](#).

Você também pode criar uma AMI em seu próprio computador Windows. Para obter mais informações, consulte os seguintes serviços:

- [AWS Server Migration Service](#)
- [VM Import/Export](#)

Manter suas AMIs atualizadas

AWSA fornece AMIs do Windows atualizadas e totalmente corrigidas em cinco dias úteis após a terça-feira de patches da Microsoft (a segunda terça-feira de cada mês). Para obter mais informações, consulte [Detalhes sobre versões de AMI do Windows da AWS \(p. 31\)](#).

As AMIs do Windows da AWS contêm as atualizações de segurança mais recentes disponíveis no momento em que foram criadas. Para obter mais informações, consulte [Patches, atualizações de segurança e IDs de AMI \(p. 32\)](#).

Tipos de virtualização

As AMIs do usam um dos dois tipos de virtualização: máquina paravirtual (PV) ou máquina virtual de hardware (HVM). As diferenças principais entre as AMIs PV e HVM são a maneira como elas inicializam e se podem aproveitar extensões especiais de hardware para melhor performance. As AMIs do Windows são AMIs HVM.

As AMIs HVM são apresentadas com um conjunto totalmente virtualizado de hardware e inicialização ao executar o registro de inicialização mestre do dispositivo de blocos raiz da sua imagem. Esse tipo de virtualização permite a execução de um sistema operacional diretamente em uma máquina virtual, sem qualquer modificação, como se tivesse sido executada em hardware bare metal. O sistema do host Amazon EC2 emula algum ou todos os hardwares subjacentes apresentados ao guest.

Os guests HVM podem aproveitar as extensões de hardware que fornecem acesso rápido ao hardware subjacente no sistema host. As AMIs HVM são necessárias para aproveitar as maiores capacidades de rede e processamento de GPU. Para passar instruções à rede especializada e a dispositivos de GPU, o SO precisa ter acesso à plataforma de hardware nativa; a virtualização de HVM dá esse acesso.

Os guests paravirtuais tradicionalmente se saem melhor com operações de armazenamento e rede que os guests de HVM, pois podem aproveitar drivers especiais para E/S que evitaram as despesas gerais de emulação de hardware de rede e de disco, enquanto os guests HVM tiveram de converter essas instruções para o hardware emulado. Agora, os drivers PV estão disponíveis para convidados do HVM. Portanto, as instâncias do Windows podem obter vantagens de performance no armazenamento e na E/S de rede usando-os. Com esses drivers de PV em HVM, os convidados recebem performance igual ao dos guests paravirtuais.

AMIs do Windows gerenciadas pela AWS

AWSA oferece as imagens de máquina da Amazon (AMIs) gerenciadas que incluem diversas versões e configurações do Windows Server. Geralmente, as AMIs do Windows da AWS são configuradas com as

definições padrão usadas pela mídia de instalação da Microsoft. No entanto, existem personalizações. Por exemplo, as AMIs do Windows da AWS acompanham os seguintes software e drivers:

- EC2Launch v2 (Windows Server 2022)
- EC2Launch (Windows Server 2016 e 2019)
- Serviço EC2Config (por meio do Windows Server 2012 R2)
- AWS Systems Manager
- AWS CloudFormation
- AWS Tools for Windows PowerShell
- Drivers de rede (SRIOV, ENA, Citrix PV)
- Drivers de armazenamento (NVMe, AWS PV, Citrix PV)
- Drivers de gráficos (NVIDIA GPU, Elastic GPU)
- Hibernação da instância spot

Para obter informações sobre outras personalizações, consulte [AWSAMIs do Windows \(p. 29\)](#).

Sumário

- [Detalhes sobre versões de AMI do Windows da AWS \(p. 31\)](#)
 - [O que esperar em uma AMI do Windows oficial da AWS \(p. 31\)](#)
 - [Como a AWS decide quais AMIs do Windows serão oferecidas \(p. 32\)](#)
 - [Patches, atualizações de segurança e IDs de AMI \(p. 32\)](#)
 - [Versões do Canal semestral \(p. 33\)](#)
- [Alterações na configuração de AMIs do Windows da AWS \(p. 33\)](#)
- [Atualizar a instância do Windows \(p. 35\)](#)
- [Atualizar ou migrar para uma versão mais recente do Windows Server \(p. 36\)](#)
- [Assinar as notificações de AMIs do Windows \(p. 36\)](#)
- [Alterações nas AMIs do Windows Server 2016 e posterior \(p. 37\)](#)
- [Conflito de contêiner de Docker em instâncias do Windows Server 2016 \(p. 37\)](#)
- [Problema com o Hibernate Agent \(AMIs de 16 de março de 2018\) \(p. 38\)](#)

Detalhes sobre versões de AMI do Windows da AWS

O que esperar em uma AMI do Windows oficial da AWS

AWSA fornece AMIs com diversas configurações para todas as versões compatíveis do sistema operacional Windows. Para cada imagem, , AWS:

- Instala todos os patches de segurança do Windows recomendados pela Microsoft. Lançamos as imagens pouco depois dos patches mensais da Microsoft serem disponibilizados.
- Instala os drivers mais recentes para hardware da AWS, incluindo drivers de rede e de disco, o EC2WinUtil para solução de problemas e os drivers de GPU em AMIs selecionadas.
- Inclui o software auxiliar AWS, como o [EC2Config \(p. 530\)](#) para Server 2012 R2 e versões anteriores, [EC2Launch \(p. 522\)](#) para Server 2016 e 2019 ou [EC2Launch v2 \(p. 482\)](#) para Server 2022.
- Configura o Windows Time para usar o [Definir o horário para uma instância do Windows. \(p. 601\)](#).
- Faz alterações em todos os esquemas de alimentação para definir o vídeo para nunca desligar.
- Executa pequenas correções de bugs, geralmente alterações de registro de uma linha para habilitar ou desabilitar recursos encontrados para melhorar a performance na AWS.

Além dos ajustes listados acima, mantemos as AMIs o mais perto possível da instalação padrão. Isso significa que, por padrão, usamos as versões de "estoque" do PowerShell ou .NET framework, não instalamos os Recursos do Windows e geralmente não alteramos a AMI.

Como a AWS decide quais AMIs do Windows serão oferecidas

Cada AMI é testada exaustivamente antes de ser lançada para o público geral. Aprimoramos periodicamente nossas ofertas de AMI para simplificar a escolha do cliente e reduzir os custos.

- Novas ofertas de AMI são criadas para novas versões do SO. Saiba que a AWS lança as ofertas "Base", "Core/Container" e "SQL Express/Standard/Web/Enterprise" em inglês e outros idiomas usados com frequência. A principal diferença entre as ofertas Base e Core é que as ofertas Base têm um desktop/GUI, enquanto as ofertas Core são apenas a linha de comando do PowerShell. Para obter mais informações sobre o Windows Server Core, consulte <https://docs.microsoft.com/en-us/windows-server/administration/server-core/what-is-server-core>.
- Novas ofertas de AMI são criadas para oferecer suporte a novas plataformas. Por exemplo, as AMIs Deep Learning e "NVidia" foram criadas para oferecer suporte aos clientes que usam os tipos de instância com base em GPU (P2 e P3, G2 e G3 etc.).
- As AMIs menos utilizadas às vezes são removidas. Se notarmos que uma AMI específica foi executada apenas algumas vezes durante seu ciclo de vida, iremos removê-la em favor de opções mais utilizadas.

Se desejar ver alguma variante de AMI, abra um ticket de suporte com a equipe de suporte da nuvem ou forneça seu feedback por meio de [um de nossos canais estabelecidos](#).

Patches, atualizações de segurança e IDs de AMI

AWSA fornece AMIs do Windows atualizadas e totalmente corrigidas em cinco dias úteis após a terça-feira de patches da Microsoft (a segunda terça-feira de cada mês). As novas AMIs ficam disponíveis instantaneamente na página Imagens no console do Amazon EC2. As novas AMIs ficam disponíveis no AWS Marketplace e na guia Início rápido do assistente de execução de instâncias em alguns dias após seu lançamento.

Note

As instâncias iniciadas a partir das AMIs do Windows Server 2019 e versões posteriores podem exibir uma mensagem do Windows Update informando "Some settings are managed by your organization" (Algumas configurações são gerenciadas por sua organização). Essa mensagem aparece como resultado de alterações no Windows Server 2019 e não afeta o comportamento do Windows Update ou sua capacidade de gerenciar as configurações de atualização.

Para remover esse aviso, consulte ["Algumas configurações são gerenciadas pela sua organização"](#).

Para garantir que os clientes tenham as atualizações de segurança mais recentes por padrão, a AWS mantém as AMIs do Windows disponíveis por três meses. Após o lançamento de novas AMIs do Windows, a AWS torna as AMIs do Windows com mais de três meses privadas em 10 dias. Depois que uma AMI tiver se tornado privada, se você observar uma instância executada nessa AMI no console, o campo ID de AMI mostrará "Cannot load detail for ami-xxxxx" (Não é possível carregar detalhes de ami-xxxxx). Talvez você não tenha permissões para visualizá-la. Você ainda pode recuperar o ID de AMI usando a AWS CLI ou o AWS SDK.

As AMIs do Windows em cada versão têm novos IDs. Portanto, recomendamos que você elabore scripts que localizem as AMIs do Windows da AWS mais recentes por seus nomes, em vez de pelos IDs. Para obter mais informações, veja os exemplos a seguir:

- [Get-EC2ImageByName](#) (AWS Tools for Windows PowerShell)
- [Consulta da AMI do Windows mais recente usando a Systems Manager Parameter Store](#)
- [Demonstração: Como pesquisar IDs de imagem de máquina da Amazon](#) (AWS Lambda, AWS CloudFormation)

Versões do Canal semestral

A AWS fornece versões do canal semestrais do Windows Server que combinam o dimensionamento, a performance e a elasticidade da AWS com os novos recursos nas [Versões do canal semestrais do Windows Server](#).

Alterações na configuração de AMIs do Windows da AWS

As alterações a seguir se aplicam a todas as AMIs do Windows da AWS.

Limpar e preparar

Alteração	Aplica-se a
Verificar renomeações de arquivo ou reinicializações pendentes e reinicializar conforme necessário	Todas as AMIs
Excluir arquivos .dmp	Todas as AMIs
Excluir logs (logs de eventos, Systems Manager, EC2Config)	Todas as AMIs
Excluir pastas e arquivos temporários para sysprep	Todas as AMIs
Limpar histórico recente (menu Iniciar, Windows Explorer etc.)	Windows Server 2012 R2 e anteriores
Realizar varredura de vírus	Todas as AMIs
Pré-compilar assemblies do .NET enfileirados (antes de sysprep)	Todas as AMIs
Executar ferramentas de manutenção do Windows	Windows Server 2012 R2 e posteriores
Restaurar valores padrão do Internet Explorer	Todas as AMIs
Restaurar valores padrão do EC2Config	Windows Server 2012 R2 e anteriores
Definir o EC2Launch para ser executado na próxima inicialização	Windows Server 2016 e 2019
Redefinir o papel de parede do Windows	Todas as AMIs
Executar sysprep	Todas as AMIs

Instalar e configurar

Alteração	Aplica-se a
Adicionar links para o Guia do Windows do Amazon EC2	Todas as AMIs
Anexar volumes de armazenamento de instâncias aos pontos de montagem prolongados	Todas as AMIs
Instalar o atua AWS Tools for Windows PowerShell	Todas as AMIs
Instalar os scripts auxiliares do AWS CloudFormation atuais	Todas as AMIs
Instalar o EC2Config e o SSM Agent atuais	Windows Server 2012 R2 e anteriores

Alteração	Aplica-se a
Instalar o EC2Launch e o SSM Agent atuais	Windows Server 2016 e 2019
Instalar o EC2Launch v2 e o SSM Agent atuais	Windows Server 2022 e posterior
Instalar os drivers AWS PV, ENA e NVMe atuais	Windows Server 2008 R2 e posteriores
Instalar os drivers SRIOV atuais	Windows Server 2012 R2 e posteriores
Instalar o driver Citrix PV atual	Windows Server 2008 SP2 e anteriores
Instalar o driver EC2WinUtil atual	Windows Server 2008 R2 e posteriores
Instalar o PowerShell 2.0 e 3.0	Windows Server 2008 SP2 e R2
Se o Microsoft SQL Server estiver instalado:	Todas as AMIs
<ul style="list-style-type: none"> • Instalar service packs • Configurar para iniciar automaticamente • Adicionar BUILTIN\Administrators à função SysAdmin • Abrir porta TCP 1433 e porta UDP 1434 	
Aplique os seguintes hotfixes:	Windows Server 2008 SP2 e R2
<ul style="list-style-type: none"> • MS15-011 • KB2582281 • KB2634328 • KB2800213 • KB2922223 • KB2394911 • KB2780879 	
Permitir tráfego ICMP pelo firewall	Windows Server 2012 R2 e anteriores
Habilitar o compartilhamento de arquivos e impressora	Windows Server 2012 R2 e anteriores
Desabilitar RunOnce para Internet Explorer	Todas as AMIs
Habilitar o PowerShell remoto	Todas as AMIs
Configure um arquivo de paginação no volume do sistema da seguinte forma:	Todas as AMIs
<ul style="list-style-type: none"> • Windows Server 2019: gerenciado pelo sistema • Windows Server 2016: gerenciado pelo sistema • Windows Server 2012 R2: o tamanho inicial e o tamanho máximo são 8 GB • Windows Server 2012 e anterior: o tamanho inicial é 512 MB e o tamanho máximo é 8 GB 	

Alteração	Aplica-se a
Configure um arquivo adicional de paginação gerenciado pelo sistema em z:, se disponível	Windows Server 2012 R2 e anteriores
Desabilitar hibernação e excluir o arquivo de hibernação	Todas as AMIs
Definir as opções de performance para obter a melhor performance	Todas as AMIs
Definir a configuração de energia como alta performance	Todas as AMIs
Desabilitar a senha do protetor de tela	Todas as AMIs
Defina a chave de registro RealTimelUniversal	Todas as AMIs
Definir o fuso horário como UTC	Todas as AMIs
Desabilitar atualizações e notificações do Windows	Todas as AMIs
Executar o Windows Update e reinicializar até não haver atualizações pendentes	Todas as AMIs
Definir a tela em todos os esquemas de alimentação para nunca desligar	Todas as AMIs
Definir a política de execução do PowerShell como "irrestrito"	Todas as AMIs

Atualizar a instância do Windows

Depois de executar uma instância Windows, você será responsável por instalar as atualizações nela. Você pode instalar manualmente apenas as atualizações de interesse ou iniciar com uma AMI do Windows da AWS e criar uma nova instância Windows. Para obter informações sobre como encontrar as AMIs do Windows atuais da AWS, consulte [Localizar uma AMI do Windows \(p. 102\)](#).

Note

Instâncias devem ser stateless durante a atualização. Para obter mais informações, consulte [Managing Your AWS Infrastructure at Scale](#) (Como gerenciar uma infraestrutura da AWS em escala).

Para instâncias Windows, você pode instalar atualizações nos seguintes serviços ou aplicações:

- [Microsoft Windows Server](#)
- [Microsoft SQL Server](#)
- [Windows PowerShell](#)
- [Instalar a versão mais recente do EC2Launch v2 \(p. 487\)](#)
- [Instalar a versão mais recente do EC2Launch \(p. 523\)](#)
- [Instalar a versão mais recente do EC2Config \(p. 532\)](#)
- [AWS Systems Manager SSM Agent do](#)
- [Habilitar redes avançadas no Windows \(p. 1031\)](#)
- [Instalar ou atualizar drivers AWS NVMe \(p. 580\)](#)
- [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#)
- [AWS Tools for Windows PowerShell](#)
- [AWS CloudFormation scripts auxiliares](#)

Você pode reiniciar uma instância Windows depois de instalar as atualizações. Para obter mais informações, consulte [Reiniciar a instância \(p. 470\)](#).

Atualizar ou migrar para uma versão mais recente do Windows Server

Para obter informações sobre como atualizar ou migrar uma instância do Windows para uma versão mais recente do Windows Server, consulte [Atualizar uma instância do Amazon EC2 do Windows para uma versão mais recente do Windows Server. \(p. 676\)](#).

Assinar as notificações de AMIs do Windows

Para ser notificado quando novas AMIs forem lançadas ou quando AMIs lançadas anteriormente se tornarem privadas, inscreva-se em notificações usando o Amazon SNS.

Para assinar as notificações de AMIs do Windows

1. Abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. Você deve usar essa região porque as notificações do SNS nas quais está se inscrevendo foram criadas nessa região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Create subscription, faça o seguinte:
 - a. Em Topic ARN, copie e cole um dos seguintes nomes de recursos da Amazon (ARNs):
 - **arn:aws:sns:us-east-1:801119661308:ec2-windows-ami-update**
 - **arn:aws:sns:us-east-1:801119661308:ec2-windows-ami-private**

Para AWS GovCloud (US):

- arn:aws-us-gov:sns:us-gov-west-1:077303321853:ec2-windows-ami-update**
- b. Em Protocol (Protocolo), escolha Email.
 - c. Para Endpoint, digite um endereço de e-mail que você pode usar para receber as notificações.
 - d. Selecione Create subscription.
 6. Você receberá um e-mail de confirmação com a linha de assunto **AWS Notification - Subscription Confirmation**. Abra o e-mail e escolha Confirm subscription para concluir a assinatura.

Sempre que AMIs do Windows forem lançadas, enviaremos notificações aos assinantes do tópico **ec2-windows-ami-update**. Sempre que AMIs do Windows já lançadas se tornarem privadas, enviaremos notificações aos assinantes do tópico **ec2-windows-ami-private**. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações de AMIs do Windows

1. Abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. Você deve usar essa região porque as notificações do SNS foram criada nessa região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione as assinaturas e escolha Actions e Delete subscriptions. Quando solicitado a confirmar, escolha Delete.

Alterações nas AMIs do Windows Server 2016 e posterior

AWS fornece AMIs para Windows Server 2016 e posterior. Essas AMIs incluem as seguintes alterações de alto nível de AMIs anteriores do Windows:

- Para acomodar a mudança do .NET Framework para o .NET Core, o serviço EC2Config foi preferido em AMIs do Windows Server 2016 e substituído pelo EC2Launch. O EC2Launch é um pacote de scripts do Windows PowerShell que executam várias tarefas que são executadas pelo serviço EC2Config. Para obter mais informações, consulte [Configurar uma instância do Windows usando o EC2Launch \(p. 522\)](#). O EC2Launch v2 substitui o EC2Launch no Windows Server 2022 e versões posteriores. Para obter mais informações, consulte [Configurar uma instância do Windows usando o EC2Launch \(p. 522\)](#).
- Em versões anteriores das AMIs do Windows Server, você pode usar o serviço EC2Config para inserir uma instância do EC2 em um domínio e configurar a integração com o Amazon CloudWatch. No Windows Server 2016 e AMIs posteriores, é possível usar o agente do CloudWatch para configurar a integração ao Amazon CloudWatch. Para obter mais informações sobre como configurar instâncias para enviar dados de log ao CloudWatch, consulte [Coletar métricas e logs de instâncias do Amazon EC2 e servidores no local com o agente do CloudWatch](#). Para obter informações sobre como inserir uma instância do EC2 em um domínio, consulte [Join an Instance to a Domain Using the AWS-JoinDirectoryServiceDomain JSON Document](#) (Insira uma instância em um domínio usando o documento JSON AWS-JoinDirectoryServiceDomain) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

Outras diferenças

Observe essas diferenças adicionais importantes para instâncias criadas a partir das AMIs do Windows Server 2016 e posterior.

- Por padrão, o EC2Launch não inicializa volumes do EBS secundários. Você pode configurar o EC2Launch para inicializar discos automaticamente programando o script para ser executado ou chamando o EC2Launch em dados do usuário. Para conhecer o procedimento para inicializar discos usando o EC2Launch, consulte "Inicializar unidades e mapeamentos de letra de unidade" em [Configurar o EC2Launch \(p. 524\)](#).
- Se você tiver previamente habilitado a integração com CloudWatch nas suas instâncias usando um arquivo de configuração local (AWS.EC2.Windows.CloudWatch.json), você poderá configurar o arquivo para trabalhar com o SSM Agent em instâncias criadas a partir de AMIs do Windows Server 2016 e posterior.

Para obter mais informações, consulte [Windows Server](#) em Microsoft.com.

Conflito de contêiner de Docker em instâncias do Windows Server 2016

Se você executar o serviço Docker em AMIs do Windows Server 2016, o serviço será configurado para usar um valor CIDR diferente do valor de prefixo do endereço IP interno padrão. O valor padrão é 172.16.0.0/12. As AMIs do Windows Server 2016 usam 172.17.0.0/16 para evitar um conflito com a Amazon EC2 VPC/sub-rede padrão. Se você não alterar as configurações de VPC/sub-rede para suas instâncias do EC2, não precisará fazer nada. O conflito é evitado essencialmente devido a valores CIDR diferentes. Se você alterar as configurações de VPC/sub-rede, lembre-se-desses valores de prefixo de endereço IP interno e evite criar um conflito. Para obter mais informações, leia a seção a seguir:

Important

Se você pretende executar o Docker em uma instância do Windows Server 2016, crie a instância de seguinte Imagem de máquina da Amazon (AMI) ou uma AMI baseada em uma imagem com Windows_Server-2016-English-Full-Containers no nome. Caso contrário, se você usar

outra AMI do Windows Server 2016, as instâncias não serão inicializadas corretamente depois de instalar o Docker e executar o Sysprep.

Problema com o Hibernate Agent (AMIs de 16 de março de 2018)

Após a versão das AMIs do Windows de 16 de março de 2018, descobrimos um caminho sem aspas na configuração do Amazon EC2 Hibernate Agent. O agente foi incluído nas AMIs para Windows Server 2008 pelo Windows Server 2016. Esse problema não afeta as AMIs para Windows Server 2003.

AWSA removeu as AMIs do Windows de 16/03/2018. Para ser notificado quando novas AMIs do Windows estiverem disponíveis, consulte [Assinar as notificações de AMIs do Windows \(p. 36\)](#).

Para minimizar o problema, é possível usar um dos procedimentos a seguir para adicionar as aspas ausentes. Se o agente estiver sendo executado, também é necessário reiniciá-lo. De forma alternativa, é possível encerrar todas as instâncias executadas de uma AMI do Windows de 16 de março de 2018 e substituí-las pelas instâncias executadas usando uma AMI diferente.

Windows PowerShell

1. Em sua instância do Windows, abra o Windows Powershell.
2. Use o seguinte comando para atualizar a configuração, adicionando as aspas ausentes:

```
cmd /c 'sc config EC2HibernateAgent binPath=\"%ProgramFiles%\Amazon\Hibernate\EC2HibernateAgent.exe\""
```

3. Use o seguinte comando para visualizar a configuração atualizada:

```
(Get-ItemProperty -Path Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EC2HibernateAgent).ImagePath
```

Verifique se a resposta está entre aspas, como no seguinte exemplo:

```
"C:\Program Files\Amazon\Hibernate\EC2HibernateAgent.exe"
```

4. Use o seguinte comando para verificar se Status é Running:

```
Get-Service EC2HibernateAgent
```

Se o agente estiver sendo executado, é necessário reiniciá-lo usando o seguinte comando para que a alteração seja implementada:

```
Restart-Service EC2HibernateAgent
```

Prompt de comando

1. Na sua instância do Windows, abra uma janela do prompt de comando.
2. Use o seguinte comando para atualizar a configuração, adicionando as aspas ausentes:

```
sc config EC2HibernateAgent binPath=\"%ProgramFiles%\Amazon\Hibernate\EC2HibernateAgent.exe\""
```

3. Use o seguinte comando para visualizar a configuração atualizada:

```
sc qc EC2HibernateAgent
```

Verifique se o caminho em **BINARY_PATH_NAME** está entre aspas, como no seguinte exemplo:

```
"C:\Program Files\Amazon\Hibernate\EC2HibernateAgent.exe"
```

4. Use o seguinte comando para verificar se STATE é RUNNING:

```
sc query EC2HibernateAgent
```

Se o agente estiver sendo executado, é necessário reiniciá-lo usando o seguinte comando para que a alteração seja implementada:

```
sc stop EC2HibernateAgent && sc start EC2HibernateAgent
```

Criar uma AMI do Windows personalizada

Você pode executar uma instância em uma AMI do Windows existente, personalizar a instância e salvar essa configuração atualizada como uma AMI personalizada. Entre as instâncias executadas nessa AMI personalizada estão as personalizações que você fez quando criou a AMI.

Para ajudar a categorizar e gerenciar suas AMIs, você pode atribuir tags personalizadas a elas. Para obter mais informações, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

Para criar uma AMI do Linux personalizada, use o procedimento para o tipo de volume da instância. Para obter mais informações, consulte [Criar uma AMI do Linux com Amazon EBS](#) ou [Criar uma AMI do Linux com armazenamento de instâncias](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

- [Como funciona a criação de uma AMI personalizada \(p. 39\)](#)
- [Criar uma AMI do Windows em uma instância em execução \(p. 40\)](#)
- [Criar uma imagem de máquina da Amazon \(AMI\) padronizada usando o Sysprep \(p. 42\)](#)

Como funciona a criação de uma AMI personalizada

Primeiro, execute uma instância de uma AMI semelhante à AMI que você deseja criar. Você pode conectá-la à sua instância e personalizá-la. Quando a instância estiver configurada da maneira desejada, garanta a integridade de dados interrompendo a instância antes de criar uma AMI e, em seguida, crie a imagem. Registraremos automaticamente a AMI para você.

Durante o processo de criação da AMI, o Amazon EC2 cria snapshots do volume raiz de sua instância e de todos os outros volumes do EBS anexados à sua instância. Você é cobrado pelos snapshots até que você cancele o registro da AMI e exclua os snapshots. Para obter mais informações, consulte [Cancelar o registro da AMI do Windows \(p. 55\)](#). Se qualquer volume anexado à instância estiver criptografado, a nova AMI só será executada com êxito em tipos de instâncias compatíveis com a Criptografia de Amazon EBS. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).

Dependendo do tamanho dos volumes, pode levar vários minutos para que o processo de criação da AMI se complete (às vezes até 24 horas). Talvez seja mais eficaz criar snapshots de seus volumes antes de criar sua AMI. Dessa forma, apenas snapshots pequenos e incrementais precisam ser criados quando a AMI é criada, e o processo é concluído mais rapidamente (o tempo total para a criação de snapshot permanece o mesmo.) Para obter mais informações, consulte [Criar snapshots de Amazon EBS \(p. 1298\)](#).

Após a conclusão do processo, uma nova AMI e um snapshot serão criados do volume raiz da instância. Quando você executa uma instância usando a nova AMI, criamos um novo volume do EBS para o volume raiz dele usando o snapshot.

Note

Uma AMI do Windows deve ser criada de uma instância do Amazon EC2. Não há suporte para a criação de uma AMI do Windows de um snapshot do EBS.

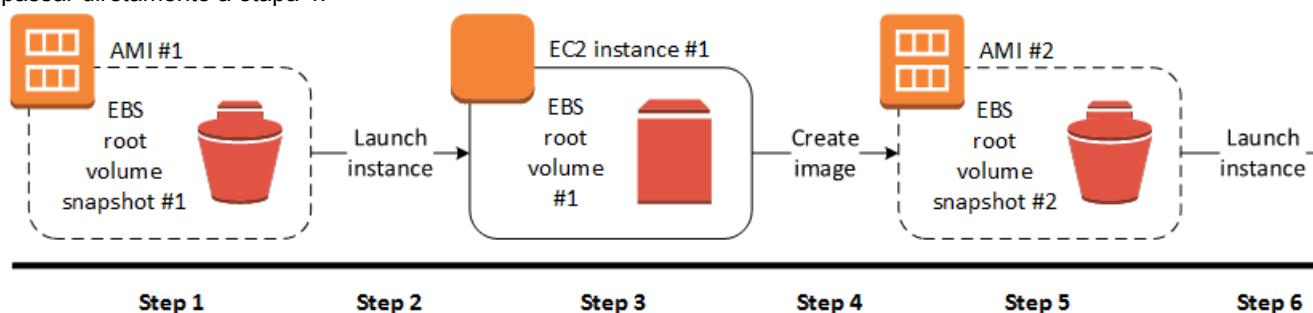
Se você adicionar volumes de armazenamento de instâncias ou volumes do Amazon Elastic Block Store (Amazon EBS) à sua instância, além do volume do dispositivo raiz, o mapeamento de dispositivos de blocos para a nova AMI conterá informações sobre esses volumes, e os mapeamentos de dispositivos de blocos para as instâncias que você executar da nova AMI conterão automaticamente informações sobre esses volumes. Os volumes de armazenamento de instâncias especificados no mapeamento de dispositivos de blocos para a nova instância são novos e não contêm dados dos volumes de armazenamento de instâncias da instância usada para criar a AMI. Os dados nos volumes do EBS persistem. Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1513\)](#).

Note

Ao criar uma nova instância em uma AMI personalizada, você deve inicializar o volume raiz e todo armazenamento do EBS adicional antes de colocá-lo em produção. Para obter mais informações, consulte [Inicializar volumes do Amazon EBS](#).

Criar uma AMI do Windows em uma instância em execução

Você pode criar uma AMI usando o AWS Management Console ou a linha de comando. O diagrama a seguir resume o processo de criação de uma AMI com base em uma instância do EC2 em execução. Comece com uma AMI existente, execute uma instância, personalize-a, crie uma nova AMI a partir dela e, por fim, execute uma instância de sua nova AMI. As etapas do diagrama a seguir são correspondentes às etapas do procedimento abaixo. Se já tiver uma instância baseada do Windows em execução, você poderá passar diretamente à etapa 4.



Para criar uma AMI de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Images (Imagens), AMIs.
3. Use as opções Filter (Filtro) para restringir o escopo da lista de AMIs às AMIs do Windows que atendam às suas necessidades. Por exemplo, para ver as AMIs do Windows fornecidas pela AWS, escolha Public images (Imagens públicas) na lista suspensa. Escolha a barra Pesquisar. Escolha Owner (Proprietário) no menu e escolha Amazon images (Imagens da Amazon). Escolha Source (Origem) no menu e digite uma das seguintes opções, dependendo da versão do Windows Server que você usa:
 - amazon/Windows_Server-2022
 - amazon/Windows_Server-2019
 - amazon/Windows_Server-2016

- amazon/Windows_Server-2012
- amazon/Windows_Server-2008

Adicione todos os outros filtros dos quais você precisa. Quando você tiver escolhido uma AMI, marque a caixa de seleção.

4. Escolha Executar. Aceite os valores padrão ao prosseguir no assistente. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#). Quando a instância estiver pronta, conecte-se a ela. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
5. Você pode executar qualquer uma destas ações em sua instância para personalizá-la de acordo com suas necessidades:

- Instalar o software e aplicações
- Copiar dados
- Reduzir o tempo de inicialização excluindo arquivos temporários, desfragmentando o disco rígido e liberando o espaço livre
- Anexar volumes adicionais do EBS
- Criar uma nova conta de usuário e a adicionar ao grupo de Administradores

Se você estiver compartilhando sua AMI, essas credenciais poderão ser fornecidas para acesso RDP sem divulgar sua senha de administrador padrão.

- [Windows Server 2022 e posterior] Defina configurações usando o EC2Launch v2. Para gerar uma senha aleatória no momento da inicialização, configure a tarefa `setAdminAccount`. Para obter mais informações, consulte [setAdminAccount \(p. 508\)](#).
 - [Windows Server 2016 e 2019] Defina configurações usando o EC2Launch. Para gerar uma senha aleatória no momento da inicialização, use a configuração `adminPasswordType`. Para obter mais informações, consulte [Configurar o EC2Launch \(p. 524\)](#).
 - [Windows Server 2012 R2 e anterior] Defina configurações usando o EC2Config. Para gerar uma senha aleatória no momento da inicialização, habilite o plug-in `Ec2SetPassword`. Do contrário, a senha de administrador atual será usada. Para obter mais informações, consulte [Arquivos de configurações do EC2Config \(p. 538\)](#).
 - [Windows Server 2008 R2] Se a instância usar drivers do RedHat para acessar o hardware virtualizado Xen, atualize para drivers do Citrix antes de criar uma AMI. Para obter mais informações, consulte [Atualizar instâncias do Windows Server 2008 e 2008 R2 \(atualização do Redhat para Citrix PV\) \(p. 569\)](#).
6. No painel de navegação, selecione Instâncias e selecione sua instância. Escolha Actions (Ações), Image and templates (Imagem e modelos) e Create image (Criar imagem).

Tip

Se essa opção está desabilitada, sua instância não é uma instância baseada em Amazon EBS.

7. Especifique um nome exclusivo para a imagem e uma descrição opcional (até 255 caracteres).

Por padrão, o Amazon EC2 encerra a instância, faz snapshots dos volumes anexados, cria e registra a AMI e, em seguida, reinicializa a instância. Escolha No reboot (Sem reinicialização) se não quiser que a instância seja encerrada.

Warning

Se você escolher No reboot (Sem reinicialização), não podemos garantir a integridade do sistema de arquivos da imagem criada.

(Opcional) Modifique o volume raiz, os volumes do EBS e os volumes de armazenamento de instâncias conforme necessário. Por exemplo:

- Para alterar o tamanho do volume raiz, localize o volume Root (Raiz) na coluna Type (Tipo) e preencha o campo Size (Tamanho).
- Para excluir um volume do EBS especificado pelo mapeamento de dispositivos de blocos da AMI usada para executar a instância, localize o volume do EBS na lista e escolha Delete (Excluir).
- Para adicionar um volume do EBS, escolha Add New Volume (Adicionar novo volume), Type (Tipo) e EBS e preencha os campos. Quando você executa uma instância da nova AMI, esses volumes adicionais são anexados automaticamente à instância. Os volumes vazios devem ser formatados e montados. Os volumes baseados em um snapshot devem ser montados.
- Para excluir um volume de armazenamento de instâncias especificado pelo mapeamento de dispositivos de blocos da AMI usada para executar a instância, localize o volume na lista e escolha Delete (Excluir).
- Para adicionar um volume de armazenamento de instâncias, escolha Add New Volume (Adicionar novo volume), Type (Tipo) e Instance Store (Armazenamento de instâncias), e selecione um nome de dispositivo na lista Device (Dispositivo). Quando você executa uma instância da nova AMI, esses volumes adicionais são automaticamente inicializados e montados. Esses volumes não contêm dados de volumes de armazenamento de instâncias da instância em execução na qual a AMI foi baseada.

Quando terminar, escolha Create Image (Criar imagem).

8. Enquanto a AMI estiver sendo criada, você poderá escolher AMIs no painel de navegação para visualizar o status. Inicialmente, ele é pending. Após alguns minutos, o status deverá mudar para available.
(Opcional) Escolha Snapshots no painel de navegação para visualizar o snapshot que foi criado para a nova AMI. Quando você executa uma instância dessa AMI, usamos esse snapshot para criar seu volume do dispositivo raiz.
9. Execute uma instância da nova AMI. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#). A nova instância em execução contém todas as personalizações aplicadas por você em etapas anteriores e todas as personalizações adicionais adicionadas por você ao executar a instância, como dados do usuário (scripts executados quando a instância é iniciada).

Para criar uma AMI de uma instância usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [create-image](#) (AWS CLI)
- [New-EC2Image](#) (AWS Tools for Windows PowerShell)

Criar uma imagem de máquina da Amazon (AMI) padronizada usando o Sysprep

A ferramenta Microsoft System Preparation (Sysprep) simplifica o processo de duplicar uma instalação personalizada do Windows. É possível usar o Sysprep para criar uma imagem de máquina da Amazon (AMI) padronizada. Você pode criar novas instâncias do Amazon EC2 para o Windows a partir desta imagem padronizada.

Recomendamos que você use o [EC2 Image Builder](#) para automatizar a criação, o gerenciamento e a implantação de imagens de servidor “douradas” personalizadas, seguras e atualizadas que são pré-instaladas e pré-configuradas com software e configurações.

Se você usar o Sysprep para criar uma AMI padronizada, recomendamos executar o Sysprep com o [EC2Launch v2 \(p. 482\)](#). Se você ainda estiver usando os agentes EC2Config (Windows Server 2012 R2 e anterior) ou EC2Launch (Windows Server 2016 e 2019), consulte a documentação para usar o Sysprep com o EC2Config e o EC2Launch a seguir.

Important

Não use o Sysprep para criar um backup da instância. O Sysprep remove informações específicas do sistema; remover essas informações pode ter consequências não intencionais para um backup da instância.

Para solucionar problemas do Sysprep, consulte [Solucionar problemas do Sysprep \(p. 1605\)](#).

Tópicos

- [Antes de começar \(p. 43\)](#)
- [Usar o Sysprep com o EC2Launch v2 \(p. 43\)](#)
- [Usar o Sysprep com o EC2Launch \(p. 46\)](#)
- [Usar o Sysprep com o EC2Config \(p. 50\)](#)

Antes de começar

- Antes de executar o Sysprep, recomendamos que você remova todas as contas de usuário locais e todos os perfis de conta, exceto a única conta de administrador em que o Sysprep será executado. Se você executar Sysprep com contas e perfis adicionais, um comportamento inesperado poderá acontecer, incluindo perda de dados de perfil ou falha de conclusão do Sysprep.
- Saiba mais sobre o [Sysprep](#) no Microsoft TechNet.
- Saiba quais [funções do servidor são compatíveis com Sysprep](#).

Usar o Sysprep com o EC2Launch v2

Esta seção contém detalhes sobre as diferentes fases de execução do Sysprep e as tarefas executadas pelo serviço EC2Launch v2 à medida que a imagem é preparada. Ele também inclui as etapas para criar uma AMI padronizada usando o Sysprep com o serviço EC2Launch v2.

Sysprep com tópicos do EC2Launch v2

- [Fases do Sysprep \(p. 43\)](#)
- [Ações do Sysprep \(p. 44\)](#)
- [Após Sysprep \(p. 46\)](#)
- [Executar o Sysprep com o EC2Launch v2 \(p. 46\)](#)

Fases do Sysprep

O Sysprep é executado nas seguintes fases:

- Generalizar: a ferramenta elimina informações e configurações específicas da imagem. Por exemplo, o Sysprep remove o identificador de segurança (SID), o nome do computador, os logs de evento e os drivers específicos, entre outros. Após essa fase ser encerrada, o sistema operacional (SO) estará pronto para criar a AMI.

Note

Ao executar o Sysprep com o serviço EC2Launch v2, o sistema impede que os drivers sejam removidos porque, por padrão, a configuração `PersistAllDeviceInstalls` é definida como `true`.

- Especializar: o plug and play examina o computador e instala drivers para todos os dispositivos detectados. A ferramenta gera requisitos do sistema operacional, como o nome de computador e o SID. Opcionalmente, você pode executar comandos nessa fase.
- Experiência Out-of-Box (OOBE): o sistema executa uma versão abreviada da configuração do Windows e pede para o usuário inserir informações como o idioma do sistema, o fuso horário e a organização registrada. Quando você executa o Sysprep com o EC2Launch v2, o arquivo de resposta automatiza essa fase.

Ações do Sysprep

O Sysprep e o EC2Launch v2 executam as seguintes ações ao preparar uma imagem.

1. Quando você escolhe Shutdown with Sysprep (Desligar com Sysprep) na caixa de diálogo EC2Launch settings (Configurações do EC2Launch), o sistema executa o comando `ec2launchn sysprep`.
2. O EC2Launch v2 edita o conteúdo do arquivo `unattend.xml` lendo o valor do registro em `HKEY_USERS\ .DEFAULT\Control Panel\International\LocaleName`. O arquivo está localizado no seguinte diretório: `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. O sistema executa o `BeforeSysprep.cmd`. Esse comando cria uma chave de registro da seguinte maneira:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f
```

A chave de registro desabilita as conexões RDP até serem re-habilitadas. Desabilitar as conexões RDP é uma medida de segurança necessária, pois, na primeira sessão de inicialização após o Sysprep ser executado, há um breve período no qual a RDP permite conexões e senha do Administrador fica em branco.

4. O serviço EC2Launch v2 chama o Sysprep executando o seguinte comando:

```
sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml"
```

Generalizar a fase

- O EC2Launch v2 remove informações e configurações específicas da imagem, como o nome do computador e o SID. Se a instância pertencer a um domínio, ela será removida do domínio. O arquivo de resposta `unattend.xml` inclui as seguintes configurações que afetam a fase:
 - `PersistAllDeviceInstalls`: essa configuração impede que a Configuração do Windows remova e reconfigure dispositivos, o que acelera o processo de preparação de imagem, pois as AMIs da Amazon exigem a execução de determinados drivers e a nova detecção desses drivers tomaria o tempo.
 - `DoNotCleanUpNonPresentDevices`: essa configuração retém informações de plug and play para dispositivos que não estão presentes no momento.
- O Sysprep fecha o SO à medida que se prepara para criar a AMI. O sistema executa uma nova instância ou inicia a instância original.

Fase especializada

O sistema gera requisitos específicos do sistema operacional, como um nome de computador e um SID. O sistema também executa as ações a seguir com base nas configurações que você especifica no arquivo de resposta `unattend.xml`.

- `CopyProfile`: o Sysprep pode ser configurado para excluir todos os perfis de usuário, incluindo o perfil incorporado do Administrador. Essa configuração retém a conta incorporada do administrador, de forma

que todas as personalizações que você fizer nessa conta serão transferidas para a nova imagem. O valor padrão é `True`.

`CopyProfile` substitui o perfil padrão pelo perfil de administrador local existente. Todas as contas em que você faz login depois da execução do Sysprep recebem uma cópia desse perfil e de seu conteúdo no primeiro login.

Se você não tiver personalizações específicas do perfil do usuário que deseja transferir para a nova imagem, altere essa configuração para `False`. O Sysprep removerá todos os perfis de usuário (isso economiza tempo e espaço em disco).

- `TimeZone`: o fuso horário é definido como Coordinated Universal Time (UTC – Tempo universal coordenado), por padrão.
- Comando síncrono com pedido 1: o sistema executa o comando a seguir, que habilita a conta do administrador e especifica o requisito de senha:

```
net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /  
PASSWORDREQ:YES
```

- Comando síncrono com pedido 2: o sistema vasculha a senha do administrador. Essa medida de segurança é projetada para impedir que a instância fique acessível após o Sysprep ser concluído, caso você não tenha habilitado a configuração `ec2setpassword`.

```
C:\Program Files\Amazon\Ec2ConfigService\ScramblePassword.exe" -u Administrator
```

- Comando síncrono com pedido 3: o sistema executa o seguinte comando:

```
C:\Program Files\Amazon\Ec2ConfigService\Scripts\SysprepSpecializePhase.cmd
```

Esse comando adiciona a seguinte chave de registro, que re-habilita a RDP:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v  
fDenyTSConnections /t REG_DWORD /d 0 /f
```

Fase OOBE

1. O sistema especifica as seguintes configurações usando o arquivo de resposta do EC2Launch v2:
 - `<InputLocale>en-US</InputLocale>`
 - `<SystemLocale>en-US</SystemLocale>`
 - `<UILanguage>en-US</UILanguage>`
 - `<UserLocale>en-US</UserLocale>`
 - `<HideEULAPage>true</HideEULAPage>`
 - `<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>`
 - `<ProtectYourPC>3</ProtectYourPC>`
 - `<BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>`
 - `<TimeZone>UTC</TimeZone>`
 - `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`
 - `<RegisteredOwner>EC2</RegisteredOwner>`

Note

Durante as fases de generalização e de especialização, o EC2Launch v2 monitora o status do sistema operacional. Se o EC2Launch v2 detectar que o sistema operacional está na fase Sysprep, ele publicará a seguinte mensagem no log do sistema:

O Windows está sendo configurado. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. O sistema executa o EC2Launch v2.

Após Sysprep

Após a conclusão do Sysprep, o EC2Launch v2 envia a seguinte mensagem para a saída do console:

```
Windows sysprep configuration complete.
```

Depois, o EC2Launch v2 executa as ações a seguir:

1. Lê o conteúdo do arquivo `agent-config.yml` e executa as tarefas configuradas.
2. Executa todas as tarefas no estágio `preReady`.
3. Após a conclusão, envia uma mensagem `Windows is ready` para os logs do sistema de instância.
4. Executa todas as tarefas no estágio `PostReady`.

Para obter mais informações sobre o EC2Launch v2, consulte [Configurar uma instância do Windows usando o EC2Launch v2 \(p. 482\)](#).

Executar o Sysprep com o EC2Launch v2

Use o procedimento a seguir para criar uma AMI padronizada usando o Sysprep com o EC2Launch v2.

1. No console do Amazon EC2, localize ou [crie \(p. 39\)](#) a AMI que deseja duplicar.
2. Execute e conecte-se à sua instância do Windows.
3. Personalize-a.
4. No menu Start (Iniciar) do Windows, procure e escolha Amazon EC2Launch settings (Configurações do Amazon EC2Launch). Para obter mais informações sobre as opções e configurações na caixa de diálogo Amazon EC2Launch settings (Configurações do Amazon EC2Launch), consulte [Configurações do EC2Launch v2 \(p. 491\)](#).
5. Selecione Shutdown with Sysprep (Desligar com Sysprep) ou Shutdown without Sysprep (Desligar sem Sysprep).

Quando houver uma solicitação para confirmar que você deseja executar o Sysprep e desativar a instância, clique em Yes (Sim). EC2Launch v2 executa o Sysprep. Você é desconectado da instância, e a instância é desligada. Se você verificar a página Instances (Instâncias) no console do Amazon EC2, o estado da instância será alterado de `Running` para `Stopping` e para `Stopped`. Nesse momento, é seguro criar uma AMI com base nessa instância.

Você pode invocar manualmente a ferramenta Sysprep pela linha de comando usando o seguinte comando:

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Usar o Sysprep com o EC2Launch

O EC2Launch oferece um arquivo de resposta padrão e arquivos em lote para o Sysprep que automatizam e protegem o processo de preparação de imagem na AMI. A modificação desses arquivos é opcional. Esses arquivos estão localizados no seguinte diretório por padrão: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.

Important

Não use o Sysprep para criar um backup da instância. O Sysprep remove as informações específicas ao sistema. Se você remover essas informações, poderá haver consequências não intencionais em um backup da instância.

Sysprep com tópicos do EC2Launch

- [Arquivos de resposta e em lotes do EC2Launch para o Sysprep \(p. 47\)](#)
- [Executar o Sysprep com o EC2Launch \(p. 47\)](#)
- [Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada \(p. 50\)](#)

[Arquivos de resposta e em lotes do EC2Launch para o Sysprep](#)

O arquivo de resposta e os arquivos em lote do EC2Launch para o Sysprep incluem o seguinte:

`Unattend.xml`

Esse é o arquivo de resposta padrão. Se você executar o `SysprepInstance.ps1` ou escolher `ShutdownWithSysprep` na interface do usuário, o sistema lerá a configuração nesse arquivo.

`BeforeSysprep.cmd`

Personalize esse arquivo em lote para executar comandos antes que o EC2Launch execute o Sysprep.

`SysprepSpecialize.cmd`

Personalize esse arquivo em lotes para executar comandos durante a fase de especialização do Sysprep.

[Executar o Sysprep com o EC2Launch](#)

Na instalação completa do Windows Server 2016 e posterior (com uma experiência de desktop), você pode executar o Sysprep com o EC2Launch manualmente ou usar a aplicação EC2 Launch Settings (Configurações de execução do EC2).

Para executar o Sysprep usando a aplicação de configurações do EC2Launch

1. No console do Amazon EC2, localize ou crie uma AMI do Windows Server 2016 ou posterior.
2. Execute uma instância do Windows a partir da AMI.
3. Conecte-se à sua instância do Windows e personalize-a.
4. Pesquise e execute a aplicação `EC2LaunchSettings`. Por padrão, ele está localizado no seguinte diretório: `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.

Ec2 Launch Settings

General

Set Computer Name

Set the computer name of the instance ip-<hex internal IP>. Disable this feature to persist your own computer name setting.

Set Wallpaper

Overlay instance information on the current wallpaper.

Extend Boot Volume

Extend OS partition to consume free space for boot volume.

Add DNS Suffix List

Add DNS suffix list to allow DNS resolution of servers running in EC2 without providing the fully qualified domain name.

Handle User Data

Execute user data provided at instance launch.
Note: This will be re-enabled when running shutdown with sysprep below.

Administrator Password

Random (Retrieve from console)

Specify (Temporarily store in config file)

Do Nothing (Customize Unattend.xml for sysprep)

These changes will take effect on next boot if Ec2Launch script is scheduled. By default, it is scheduled by shutdown options below.

Sysprep

Sysprep is a Microsoft tool that prepares an image for multiple launches.

Ec2Launch Script Location: [Found](#)

`C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInsta`

Run EC2Launch on every boot (instead of just the next boot).

5. Selecione ou limpe as opções conforme for necessário. Essas configurações são armazenadas no arquivo `LaunchConfig.json`.
6. Em `Administrator password`, faça uma das seguintes ações:
 - Escolha Random. O EC2Launch gera uma senha e criptografa-a usando a chave de usuário. O sistema desativa essa configuração depois da execução da instância, portanto, essa senha persistirá se a instância for reinicializada ou parada e iniciada.
 - Escolha Specify e digite a senha que atende aos requisitos do sistema. A senha é armazenada em `LaunchConfig.json` como texto não criptografado e será excluída depois que Sysprep definir a senha do administrador. Se você fechar agora, a senha será definida imediatamente. O EC2Launch criptografa a senha usando a chave de usuário.
 - Escolha DoNothing e especifique uma senha no arquivo `unattend.xml`. Se você não especificar uma senha em `unattend.xml`, a conta de administrador ficará desativada.
7. Escolha Shutdown with Sysprep (Desligar com Sysprep).

Para usar o Sysprep manualmente usando o EC2Launch

1. No console do Amazon EC2, localize ou crie uma AMI Datacenter Edition do Windows Server 2016 ou posterior que você deseja duplicar.
2. Execute e conecte-se à sua instância do Windows.
3. Personalize a instância.
4. Especifique as configurações no arquivo `LaunchConfig.json`. Por padrão, esse arquivo está localizado no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para `adminPasswordType`, especifique um dos seguintes valores:

`Random`

O EC2Launch gera uma senha e criptografa-a usando a chave de usuário. O sistema desativa essa configuração depois da execução da instância, portanto, essa senha persistirá se a instância for reinicializada ou parada e iniciada.

`Specify`

O EC2Launch usa a senha que você especifica `adminPassword`. Se a senha não atender aos requisitos de sistema, o EC2Launch gera uma senha aleatória. A senha é armazenada em `LaunchConfig.json` como texto não criptografado e será excluída depois que Sysprep definir a senha do administrador. O EC2Launch criptografa a senha usando a chave de usuário.

`DoNothing`

O EC2Launch usa a senha que você especifica o arquivo `unattend.xml`. Se você não especificar uma senha em `unattend.xml`, a conta de administrador ficará desativada.

5. (Opcional) Especifique as configurações em `unattend.xml` e em outros arquivos de configuração. Se o plano atender à instalação, você não precisará fazer alterações nesses arquivos. Por padrão, os arquivos estão localizados no seguinte diretório: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. No Windows PowerShell, execute `./InitializeInstance.ps1 -Schedule`. Por padrão, o script está localizado no seguinte diretório: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`. Esse script agenda a instância para ser inicializada durante a próxima inicialização. Você deve executar esse script antes de executar o script `SysprepInstance.ps1` na próxima etapa.
7. No Windows PowerShell, execute `./sysprepInstance.ps1`. Por padrão, o script está localizado no seguinte diretório: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Você é desconectado da instância, e a instância é encerrada. Se você verificar a página Instances (Instâncias) no console do Amazon EC2, o estado da instância será alterado de Running para Stopping e, em seguida, para Stopped. Nesse momento, é seguro criar uma AMI com base nessa instância.

[Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada](#)

Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada, siga estas etapas:

- Execute a GUI EC2LaunchSettings (C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\EC2LaunchSettings.exe) e selecione a opção para encerrar com o Sysprep.
- Execute EC2LaunchSettings e desligue sem o Sysprep antes de criar a AMI. Isso configura as tarefas de inicialização do EC2 para serem executadas na próxima inicialização, que definirá as rotas com base na sub-rede da instância.
- Reprograme manualmente as tarefas de inicialização do EC2 antes de criar uma AMI do [PowerShell \(p. 524\)](#).

Important

Observe o comportamento padrão de redefinição de senha antes de reprogramar as tarefas.

- Para atualizar as rotas em uma instância em execução que está passando por ativação do Windows ou comunicação com falhas de metadados de instância, consulte “[Não é possível ativar o Windows](#)” (p. 1642).

[Usar o Sysprep com o EC2Config](#)

Esta seção contém os detalhes das diferentes fases de execução do Sysprep e das tarefas executadas pelo serviço EC2Config enquanto a imagem é preparada. Ela também inclui as etapas para criar uma AMI padronizada usando o Sysprep com o serviço EC2Config.

Sysprep com tópicos EC2Config

- [Fases do Sysprep \(p. 43\)](#)
- [Ações do Sysprep \(p. 51\)](#)
- [Após Sysprep \(p. 53\)](#)
- [Executar o Sysprep com o serviço EC2Config \(p. 54\)](#)

[Fases do Sysprep](#)

O Sysprep é executado nas seguintes fases:

- Generalizar: a ferramenta elimina informações e configurações específicas da imagem. Por exemplo, o Sysprep remove o identificador de segurança (SID), o nome do computador, os logs de evento e os drivers específicos, entre outros. Após essa fase ser encerrada, o sistema operacional (SO) estará pronto para criar a AMI.

Note

Quando você executa o Sysprep com o serviço EC2Config, o sistema impede que os drivers sejam removidos, pois a configuração PersistAllDeviceInstalls é definida como verdadeira por padrão.

- Especializar: o plug and play examina o computador e instala drivers para todos os dispositivos detectados. A ferramenta gera requisitos de SO, como nome de computador e SID. Opcionalmente, você pode executar comandos nessa fase.
- Out-of-Box Experience (OOBE): o sistema executa uma versão abreviada da configuração do Windows e pede para o usuário digitar informações como idioma do sistema, fuso horário e uma organização

registrada. Quando você executa o Sysprep com o EC2Config, o arquivo de resposta automatiza essa fase.

Ações do Sysprep

O Sysprep e o serviço EC2Config executam as ações a seguir ao preparar uma imagem.

1. Quando você escolher Shutdown with Sysprep (Desativação com Sysprep) na caixa de diálogo EC2 Service Properties (Propriedades do serviço EC2), o sistema executará o comando `ec2config.exe -sysprep`.
2. O serviço EC2Config lê o conteúdo do arquivo `BundleConfig.xml`. Esse arquivo está localizado no diretório a seguir, por padrão: `C:\Program Files\Amazon\Ec2ConfigService\Settings`.

O arquivo `BundleConfig.xml` inclui as seguintes configurações. Você pode alterar essas configurações:

- `AutoSysprep`: indica se o Sysprep deve ser usado automaticamente. Você não precisará mudar esse valor se estiver executando o Sysprep pela caixa de diálogo de propriedades do serviço EC2. O valor padrão é `No`.
 - `SetRDPCertificate`: define um certificado autoassinado para o servidor de Desktop Remoto. Isso permite que você use com segurança o Remote Desktop Protocol (RDP) para se conectar à instância. Altere o valor para `Yes` se as novas instâncias precisarem usar um certificado. Essa configuração não é usada com instâncias do Windows Server 2008 ou Windows Server 2012, pois esses sistemas operacionais podem gerar seus próprios certificados. O valor padrão é `No`.
 - `SetPasswordAfterSysprep`: define uma senha aleatória em uma instância recém-executada, criptografa-a com a chave de execução do usuário e gera a senha criptografada no console. Altere o valor para `No` se novas instâncias não precisarem ser definidas com uma senha criptografada aleatória. O valor padrão é `Yes`.
 - `PreSysprepRunCmd`: o local do comando para execução. Por padrão, o comando está localizado no seguinte diretório: `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`
3. O sistema executa o `BeforeSysprep.cmd`. Esse comando cria uma chave de registro da seguinte maneira:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f
```

A chave de registro desabilita as conexões RDP até serem re-habilitadas. Desabilitar as conexões RDP é uma medida de segurança necessária, pois, na primeira sessão de inicialização após o Sysprep ser executado, há um breve período no qual a RDP permite conexões e senha do Administrador fica em branco.

4. O serviço EC2Config chama o Sysprep executando o seguinte comando:

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /oobe /generalize /shutdown
```

Generalizar a fase

- A ferramenta remove informações específicas da imagem e as configurações, como nome de computador e SID. Se a instância pertencer a um domínio, ela será removida do domínio. O arquivo de resposta `sysprep2008.xml` inclui as seguintes configurações que afetam a fase:
 - `PersistAllDeviceInstalls`: essa configuração impede que a Configuração do Windows remova e reconfigure dispositivos, o que acelera o processo de preparação de imagem, pois as AMIs da

Amazon exigem a execução de determinados drivers e a nova detecção desses drivers tomaria o tempo.

- DoNotCleanUpNonPresentDevices: essa configuração retém informações de plug and play para dispositivos que não estão presentes no momento.
- O Sysprep fecha o SO à medida que se prepara para criar a AMI. O sistema executa uma nova instância ou inicia a instância original.

Fase especializada

O sistema gera requisitos específicos de SO, como um nome de computador e um SID. O sistema também executa as ações a seguir com base em configurações que você especifica no arquivo de resposta sysprep2008.xml.

- CopyProfile: o Sysprep pode ser configurado para excluir todos os perfis de usuário, incluindo o perfil incorporado do Administrador. Essa configuração retém a conta de Administrador incorporada, de forma que todas as personalizações que você fizer nessa conta serão transferidas para a nova imagem. O valor padrão é Verdadeiro.

CopyProfile substitui o perfil padrão pelo perfil de administrador local existente. Todas as contas conectadas depois da execução de Sysprep receberão uma cópia desse perfil e do conteúdo no primeiro login.

Se você não tiver personalizações específicas do perfil do usuário que deseja transferir para a nova imagem, altere essa configuração para falso. O Sysprep removerá todos os perfis de usuário; isso economiza tempo e espaço em disco.

- TimeZone: o fuso horário é definido como Coordinated Universal Time (UTC – Tempo universal coordenado), por padrão.
- Comando síncrono com pedido 1: o sistema executa o comando a seguir, que habilita a conta do administrador e especifica o requisito de senha.

```
net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /  
PASSWORDREQ:YES
```

- Comando síncrono com pedido 2: o sistema vasculha a senha do administrador. Essa medida de segurança é projetada para impedir que a instância fique acessível após o Sysprep ser concluído, caso você não tenha habilitado a configuração ec2setpassword.

```
C:\Program Files\Amazon\Ec2ConfigService\ScramblePassword.exe" -u Administrator
```

- Comando síncrono com pedido 3: o sistema executa o seguinte comando:

```
C:\Program Files\Amazon\Ec2ConfigService\Scripts\SysprepSpecializePhase.cmd
```

Esse comando adiciona a seguinte chave de registro, que re-habilita a RDP:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v  
fDenyTSConnections /t REG_DWORD /d 0 /f
```

Fase OOBE

1. Usando o arquivo de resposta do serviço EC2Config, o sistema especifica as seguintes configurações:

- <InputLocale>en-US</InputLocale>
- <SystemLocale>en-US</SystemLocale>
- <UILanguage>en-US</UILanguage>
- <UserLocale>en-US</UserLocale>
- <HideEULAPage>true</HideEULAPage>

- <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
- <NetworkLocation>Other</NetworkLocation>
- <ProtectYourPC>3</ProtectYourPC>
- <BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>
- <TimeZone>UTC</TimeZone>
- <RegisteredOrganization>Amazon.com</RegisteredOrganization>
- <RegisteredOwner>Amazon</RegisteredOwner>

Note

Durante as fases de generalização e especialização, o serviço EC2Config monitora o status do SO. Se o EC2Config detectar que o sistema operacional está na fase Sysprep, ele publicará a seguinte mensagem no log do sistema:

EC2ConfigMonitorState: 0 O Windows está sendo configurado.

SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Após a conclusão da fase OOBE, o sistema executa `SetupComplete.cmd` a partir do seguinte local: `C:\Windows\Setup\Scripts\SetupComplete.cmd`. Na AMIs públicas da Amazon antes de abril de 2015 este arquivo estava vazio e não executava nada na imagem. Em AMIs públicas posteriores a abril de 2015, o arquivo inclui o seguinte valor: call "C:\Program Files\Amazon\Ec2ConfigService\Scripts\PostSysprep.cmd".
3. O sistema executa `PostSysprep.cmd`, que realiza as seguintes operações:
 - Define a senha do Administrador para não expirar. Se a senha expirou, os Administradores podem não conseguir fazer login.
 - Define o nome da máquina MSSQLServer (se instalada) para que o nome esteja em sincronia com a AMI.

Após Sysprep

Após o Sysprep ser concluído, os serviços do EC2Config enviam a seguinte mensagem para a saída do console:

```
Windows sysprep configuration complete.  
Message: Sysprep Start  
Message: Sysprep End
```

O EC2Config então executa as ações a seguir:

1. Lê o conteúdo do arquivo `config.xml` e lista todos os plug-ins habilitados.
2. Executa todos os plug-ins "Antes que o Windows esteja pronto" ao mesmo tempo.
 - Ec2SetPassword
 - Ec2SetComputerName
 - Ec2InitializeDrives
 - Ec2EventLog
 - Ec2ConfigureRDP
 - Ec2OutputRDPCert
 - Ec2SetDriveLetter
 - Ec2WindowsActivate
 - Ec2DynamicBootVolumeSize
3. Após estar concluído, envia uma mensagem "O Windows está pronto" para os logs do sistema de instância.
4. Executa todos os plug-ins "Após o Windows estar pronto" ao mesmo tempo.

- Amazon CloudWatch Logs
- UserData
- AWS Systems Manager (Systems Manager)

Para obter mais informações sobre plug-ins do Windows, consulte [Configurar uma instância do Windows usando o serviço EC2Config \(p. 530\)](#).

Executar o Sysprep com o serviço EC2Config

Use o procedimento a seguir para criar uma AMI padronizada usando Sysprep e serviço EC2Config.

1. No console do Amazon EC2, localize ou [crie \(p. 39\)](#) a AMI que deseja duplicar.
2. Execute e conecte-se à sua instância do Windows.
3. Personalize-a.
4. Especifique as definições de configuração no arquivo de resposta do serviço EC2Config:

```
C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml
```
5. No menu Iniciar do Windows, escolha Todos os Programas e Configurações do EC2ConfigService.
6. Escolha a guia Image (Imagen) na caixa de diálogo Ec2 Service Properties (Propriedades do serviço Ec2). Para obter mais informações sobre as opções e as configurações da caixa de diálogo Ec2 Service Properties (Propriedades do serviço Ec2), consulte [Propriedades do serviço Ec2 \(p. 530\)](#).
7. Selecione uma opção para a senha do Administrador e selecione Shutdown with Sysprep (Desativação com Sysprep) ou Shutdown without Sysprep (Desativação sem Sysprep). O EC2Config edita os arquivos de configuração com base na opção de senha selecionada.
 - Random (Aleatório): o EC2Config gera uma senha, criptografa-a com a chave do usuário e exibe a senha criptografada no console. Nós desabilitamos essa configuração depois da primeira execução, de forma que essa senha persistirá se a instância for reinicializada ou parada e inicializada.
 - Specify (Especificar): a senha é armazenada no arquivo de resposta do Sysprep de forma não criptografada (texto aberto). Quando o Sysprep é executado em seguida, ele define a senha do Administrador. Se você fechar agora, a senha será definida imediatamente. Quando o serviço é reiniciado novamente, a senha do Administrador é removida. É importante recordar essa senha, pois você não poderá recuperá-la depois.
 - Keep Existing (Manter existente): a senha existente para a conta do Administrador não muda quando o Sysprep é executado ou o EC2Config é reiniciado. É importante recordar essa senha, pois você não poderá recuperá-la depois.
8. Escolha OK.

Quando houver uma solicitação para confirmar que você deseja executar o Sysprep e desativar a instância, clique em Yes (Sim). Você verá que o EC2Config executa Sysprep. Em seguida, você é desconectado da instância e a instância é desligada. Se você verificar a página Instances (Instâncias) no console do Amazon EC2, o estado da instância mudará de Running para Stopping e, finalmente, para Stopped. Nesse momento, é seguro criar uma AMI com base nessa instância.

Você pode invocar manualmente a ferramenta Sysprep pela linha de comando usando o seguinte comando:

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep"
```

Note

As aspas duplas no comando não serão necessárias se o shell do seu CMD já estiver no diretório C:\Program Files\Amazon\EC2ConfigService\.

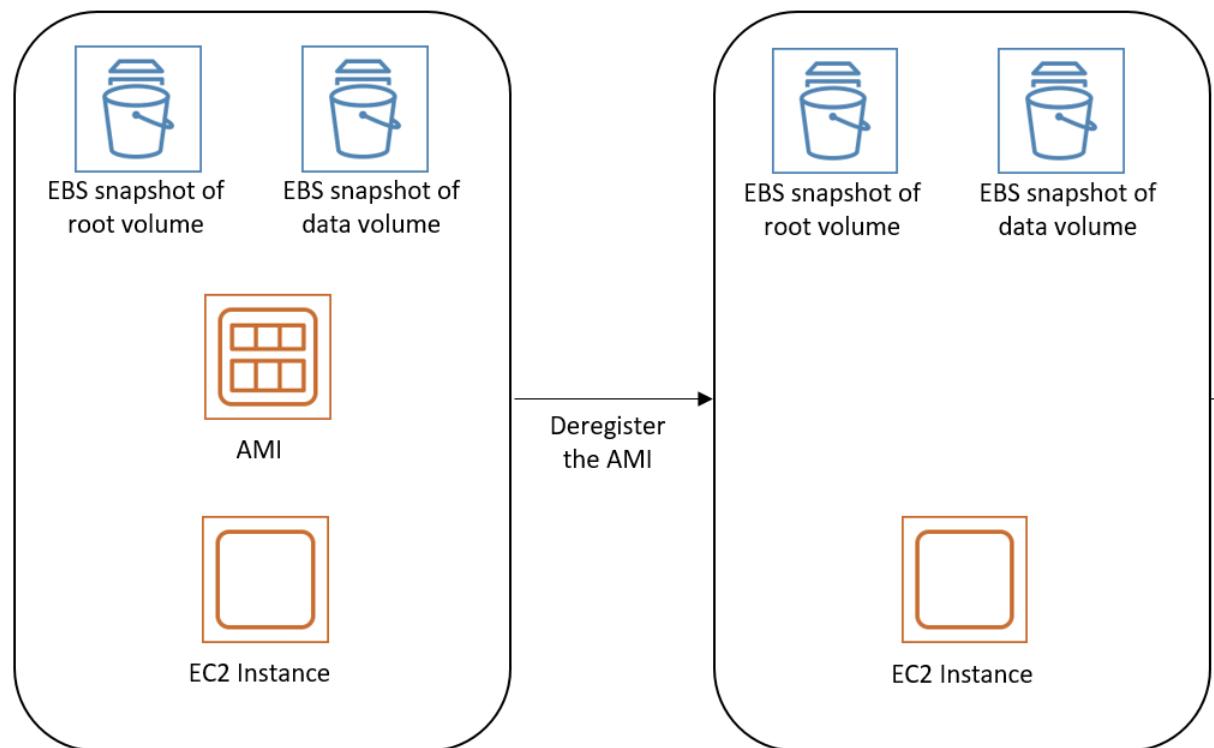
Contudo, você deve ser muito cuidadoso para que as opções do arquivo XML especificadas na pasta `Ec2ConfigService\Settings` estejam corretas; caso contrário, pode não conseguir conectar-se à instância. Para obter mais informações sobre os arquivos de configurações, consulte [Arquivos de configurações do EC2Config \(p. 538\)](#). Para ver um exemplo de como configurar e executar o Sysprep pela linha de comando, consulte `Ec2ConfigService\Scripts\InstallUpdates.ps1`.

Cancelar o registro da AMI do Windows

Você pode cancelar o registro de uma AMI do Windows quando tiver terminado de usá-la. Depois de cancelar o registro de uma AMI, você não poderá usá-la para executar novas instâncias.

Quando o registro da AMI é cancelado, isso não afeta nenhuma instância já executada a partir da AMI nem snapshots criados durante o processo de criação da AMI. Você continuará assumindo os custos de uso dessas instâncias e custos de armazenamento do snapshot. Portanto, você deve encerrar todas as instâncias que não serão mais usadas, assim como excluir os snapshots que não serão mais usados.

O diagrama a seguir ilustra o processo para limpar a AMI do Windows.



Para limpar sua AMI do Windows

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione AMIs. Selecione a AMI e anote o seu ID — isso pode ajudá-lo a encontrar o snapshot correto na próxima etapa. Escolha Actions (Ações) e, em seguida, Deregister (Cancelar o registro). Quando solicitada a confirmação, selecione Continue (Continuar).

Note

O console pode demorar alguns minutos para remover a AMI da lista. Escolha Refresh (Atualizar) para atualizar o status.

3. No painel de navegação, selecione Snapshots e selecione o snapshot (procure o ID da AMI na coluna Description (Descrição)). Escolha Actions (Ações) e, em seguida, escolha Delete Snapshot (Excluir snapshot). Quando a confirmação for solicitada, escolha Yes, Delete (Sim, excluir).
4. (Opcional) Se você tiver terminado de trabalhar com uma instância executada pela AMI, encerre-a. No painel de navegação, escolha Instances (Instâncias). Selecione a instância e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância). Quando a confirmação for solicitada, escolha Terminate (Encerrar).

AMIs especializadas do Windows

Esta seção contém informações sobre AMIs do Windows especializadas e AMIs do Windows desenvolvidas para soluções de workload da Microsoft.

Tópicos

- [AMIs do SQL Server fornecidas pela AWS \(p. 56\)](#)
- [AMIs do Amazon EC2 Windows Server para conformidade com STIG \(p. 56\)](#)

AMIs do SQL Server fornecidas pela AWS

Para AMIs incluídas com a licença do SQL Server, use a mídia de instalação e configuração incluída c:\SQLServerSetup para fazer alterações na instalação padrão, adicionar novos recursos ou instalar instâncias nomeadas adicionais.

AMIs do Amazon EC2 Windows Server para conformidade com STIG

Guias de implementação técnica de segurança (STIGs) são os padrões de configuração criados pela agência de sistemas de informação de defesa (DISA, Defense Information Systems Agency) para proteger os sistemas e softwares de informação. Para que seus sistemas estejam em conformidade com os padrões STIG, você deve instalar, definir e testar uma variedade de configurações de segurança. As AMIs do Amazon EC2 Windows Server para conformidade com os padrões STIG são pré-configuradas com mais de 160 configurações de segurança obrigatórias. Os sistemas operacionais em conformidade com os padrões STIG incluem o Windows Server 2012 R2, Windows Server 2016 e Windows Server 2019. As AMIs em conformidade com os padrões STIG incluem certificados atualizados do departamento de defesa (DoD, Department of Defense) que ajudam você a ingressar e alcançar a conformidade com os padrões STIG. Não há cobranças adicionais pelo uso de AMIs em conformidade com os padrões STIG.

AMIs do Amazon EC2 Windows Server para conformidade com os padrões STIG estão disponíveis em todas as regiões públicas da AWS e do GovCloud. Você pode executar instâncias dessas AMIs diretamente do console do Amazon EC2. Elas são cobradas usando a definição de preço padrão do Windows.

As AMIs do Amazon EC2 compatíveis com STIG para Windows Server podem ser encontradas nas AMIs da comunidade quando você cria uma instância. Os nomes das AMIs são os seguintes:

Note

O sufixo de data da AMI (**AAA.MM.DD**) é a data em que a versão mais recente foi criada. Você pode procurar a versão sem o sufixo de data.)

- Windows_Server-2019-English-STIG-Full-**YYYY.MM.DD**

- Windows_Server-2019-English-STIG-Core-**YYYY.MM.DD**
- Windows_Server-2016-English-STIG-Full-YYYY.MM.DD
- Windows_Server-2016-English-STIG-Core-YYYY.MM.DD
- Windows_Server-2012-R2-English-STIG-Full-**YYYY.MM.DD**
- Windows_Server-2012-R2-English-STIG-Core-**YYYY.MM.DD**

Níveis de conformidade

- Alto (categoria I)

O risco mais grave. Inclui qualquer vulnerabilidade que possa resultar em perda de confidencialidade, disponibilidade ou integridade.

- Médio (categoria II)

Qualquer vulnerabilidade que possa resultar em perda de confidencialidade, disponibilidade ou integridade, mas onde os riscos podem ser mitigados.

- Baixo (categoria III)

Inclui qualquer vulnerabilidade que degrada medidas de proteção contra perda de confidencialidade, disponibilidade ou integridade.

As seções a seguir mostram os STIGs que foram aplicados a cada sistema operacional Windows e seus componentes.

Tópicos

- [Sistemas operacionais Core e Base \(p. 57\)](#)
- [Microsoft .NET Framework 4.0 STIG V2 Versão 1 \(p. 59\)](#)
- [Windows Firewall STIG V1 versão 7 \(p. 60\)](#)
- [Internet Explorer \(IE\) 11 STIG V1 Versão 19 \(p. 60\)](#)
- [Histórico de versões \(p. 61\)](#)

Sistemas operacionais Core e Base

As AMIs do Amazon EC2 compatíveis com o STIG são projetadas para uso como servidores independentes e têm o nível mais alto de configurações STIG aplicadas (Categoria 1). Cada nível de compatibilidade contém todas as configurações STIG de níveis inferiores, o que significa que o nível mais alto tem todas as configurações aplicáveis de todos os níveis.

Algumas configurações STIG não são aplicadas automaticamente. Isso pode ocorrer devido a limitações técnicas. Por exemplo, a configuração STIG pode não ser aplicável a servidores autônomos. As políticas específicas da organização também podem impedir a aplicação automática das configurações STIG, como um requisito para que os administradores revisem as configurações do documento. Para obter mais detalhes sobre quais STIGs são aplicados às AMIs do Windows do Amazon EC2, você pode fazer download de nossa [planilha](#).

Para obter uma lista completa dos STIGs do Windows, consulte a [STIGs Document Library](#). Para obter informações sobre como visualizar a lista completa, consulte [How to View SRGs and STIGs](#) (Como exibir SRGs e STIGs).

Windows Server 2019 STIG V2 Release 2

Aplicam-se todas as seguintes configurações STIG para sistemas operacionais Windows:

- Windows\Baixo

V-205691, V-205819, V-205858, V-205859, V-205860, V-205870, V-205871 e V-205923

- Windows\Médio

V-205625, V-205626, V-205627, V-205629, V-205630, V-205633, V-205634, V-205635, V-205636, V-205637, V-205638, V-205639, V-205643, V-205644, V-205648, V-205649, V-205650, V-205651, V-205652, V-205655, V-205656, V-205659, V-205660, V-205662, V-205671, V-205672, V-205673, V-205675, V-205676, V-205678, V-205679, V-205680, V-205681, V-205682, V-205683, V-205684, V-205685, V-205686, V-205687, V-205688, V-205689, V-205690, V-205692, V-205693, V-205694, V-205697, V-205698, V-205708, V-205709, V-205712, V-205714, V-205716, V-205717, V-205718, V-205719, V-205720, V-205722, V-205729, V-205730, V-205733, V-205747, V-205751, V-205752, V-205754, V-205756, V-205758, V-205759, V-205760, V-205761, V-205762, V-205764, V-205765, V-205766, V-205767, V-205768, V-205769, V-205770, V-205771, V-205772, V-205773, V-205774, V-205775, V-205776, V-205777, V-205778, V-205779, V-205780, V-205781, V-205782, V-205783, V-205784, V-205795, V-205796, V-205797, V-205798, V-205801, V-205808, V-205809, V-205810, V-205811, V-205812, V-205813, V-205814, V-205815, V-205816, V-205817, V-205821, V-205822, V-205823, V-205824, V-205825, V-205826, V-205827, V-205828, V-205830, V-205831, V-205832, V-205833, V-205834, V-205835, V-205836, V-205837, V-205838, V-205839, V-205840, V-205841, V-205861, V-205863, V-205865, V-205866, V-205867, V-205868, V-205869, V-205872, V-205873, V-205874, V-205878, V-205879, V-205880, V-205881, V-205889, V-205891, V-205905, V-205911, V-205912, V-205915, V-205916, V-205917, V-205918, V-205920, V-205921, V-205922, V-205924, V-205925 e V-236001

- Windows\Alto

V-205653, V-205654, V-205711, V-205713, V-205724, V-205725, V-205757, V-205802, V-205804, V-205805, V-205806, V-205849, V-205908, V-205913, V-205914 e V-205919

Windows Server 2016 STIG V2 Release 2

Aplicam-se todas as seguintes configurações STIG para sistemas operacionais Windows:

- Windows\Baixo

V-224916, V-224917, V-224918, V-224919, V-224931, V-224942 e V-225060

- Windows\Médio

V-224850, V-224852, V-224853, V-224854, V-224855, V-224856, V-224857, V-224858, V-224859, V-224866, V-224867, V-224868, V-224869, V-224870, V-224871, V-224872, V-224873, V-224881, V-224882, V-224883, V-224884, V-224885, V-224886, V-224887, V-224888, V-224889, V-224890, V-224891, V-224892, V-224893, V-224894, V-224895, V-224896, V-224897, V-224898, V-224899, V-224900, V-224901, V-224902, V-224903, V-224904, V-224905, V-224906, V-224907, V-224908, V-224909, V-224910, V-224911, V-224912, V-224913, V-224914, V-224915, V-224920, V-224922, V-224924, V-224925, V-224926, V-224927, V-224928, V-224929, V-224930, V-224935, V-224936, V-224937, V-224938, V-224939, V-224940, V-224941, V-224943, V-224944, V-224945, V-224946, V-224947, V-224948, V-224949, V-224951, V-224952, V-224953, V-224955, V-224956, V-224957, V-224959, V-224960, V-224962, V-224963, V-225010, V-225013, V-225014, V-225015, V-225016, V-225017, V-225018, V-225019, V-225021, V-225022, V-225023, V-225024, V-225028, V-225029, V-225030, V-225031, V-225032, V-225033, V-225034, V-225035, V-225038, V-225039, V-225040, V-225041, V-225042, V-225043, V-225047, V-225049, V-225050, V-225051, V-225052, V-225055, V-225056, V-225057, V-225058, V-225061, V-225062, V-225063, V-225064, V-225065, V-225066, V-225067, V-225068, V-225069, V-225072, V-225073, V-225074, V-225076, V-225078, V-225080, V-225081, V-225082, V-225083, V-225084, V-225086, V-225087, V-225088, V-225089, V-225092, V-225093 e V-236000

- Windows\Alto

V-224874, V-224932, V-224933, V-224934, V-224954, V-224958, V-224961, V-225025, V-225044, V-225045, V-225046, V-225048, V-225053, V-225054 e V-225079

Windows Server 2012 R2 STIG V3 Release 2

Aplicam-se todas as seguintes configurações STIG para sistemas operacionais Windows:

- Windows\Baixo

V-225537, V-225536, V-225526, V-225525, V-225514, V-225511, V-225490, V-225489, V-225488, V-225487, V-225485, V-225484, V-225483, V-225482, V-225481, V-225480, V-225479, V-225476, V-225473, V-225468, V-225462, V-225460, V-225459, V-225412, V-225394, V-225392, V-225376, V-225363, V-225362, V-225360, V-225359, V-225358, V-225357, V-225355, V-225343, V-225342, V-225336, V-225335, V-225334, V-225333, V-225332, V-225331, V-225330, V-225328, V-225327, V-225324, V-225319, V-225318 e V-225250

- Windows\Médio

V-225574, V-225573, V-225572, V-225571, V-225570, V-225569, V-225568, V-225567, V-225566, V-225565, V-225564, V-225563, V-225562, V-225561, V-225560, V-225559, V-225558, V-225557, V-225555, V-225554, V-225553, V-225551, V-225550, V-225549, V-225548, V-225546, V-225545, V-225544, V-225543, V-225542, V-225541, V-225540, V-225539, V-225538, V-225535, V-225534, V-225533, V-225532, V-225531, V-225530, V-225529, V-225528, V-225527, V-225524, V-225523, V-225522, V-225521, V-225520, V-225519, V-225518, V-225517, V-225516, V-225515, V-225513, V-225510, V-225509, V-225508, V-225506, V-225504, V-225503, V-225502, V-225501, V-225500, V-225494, V-225486, V-225478, V-225477, V-225475, V-225474, V-225472, V-225471, V-225470, V-225469, V-225464, V-225463, V-225461, V-225458, V-225457, V-225456, V-225455, V-225454, V-225453, V-225452, V-225448, V-225443, V-225442, V-225441, V-225415, V-225414, V-225413, V-225411, V-225410, V-225409, V-225408, V-225407, V-225406, V-225405, V-225404, V-225402, V-225401, V-225400, V-225398, V-225397, V-225395, V-225393, V-225391, V-225389, V-225386, V-225385, V-225384, V-225383, V-225382, V-225381, V-225380, V-225379, V-225378, V-225377, V-225375, V-225374, V-225373, V-225372, V-225371, V-225370, V-225369, V-225368, V-225367, V-225356, V-225353, V-225352, V-225351, V-225350, V-225349, V-225348, V-225347, V-225346, V-225345, V-225344, V-225341, V-225340, V-225339, V-225338, V-225337, V-225329, V-225326, V-225325, V-225323, V-225322, V-225321, V-225320, V-225317, V-225316, V-225315, V-225314, V-225305, V-225304, V-225303, V-225302, V-225301, V-225300, V-225299, V-225298, V-225297, V-225296, V-225295, V-225294, V-225293, V-225292, V-225291, V-225290, V-225289, V-225288, V-225287, V-225286, V-225285, V-225284, V-225283, V-225282, V-225281, V-225280, V-225279, V-225278, V-225277, V-225276, V-225275, V-225273, V-225272, V-225271, V-225270, V-225269, V-225268, V-225267, V-225266, V-225265, V-225264, V-225263, V-225261, V-225260, V-225259 e V-225239

- Windows\Alto

V-225556, V-225552, V-225547, V-225507, V-225505, V-225498, V-225497, V-225496, V-225493, V-225492, V-225491, V-225449, V-225444, V-225399, V-225396, V-225390, V-225366, V-225365, V-225364, V-225354 e V-225274

Microsoft .NET Framework 4.0 STIG V2 Versão 1

A lista a seguir contém configurações STIG que são aplicadas aos componentes do sistema operacional Windows para AMIs do Amazon EC2 compatíveis com o STIG. Algumas configurações STIG não são aplicadas automaticamente. Isso pode ocorrer devido a limitações técnicas. Por exemplo, a configuração STIG pode não ser aplicável a servidores autônomos. As políticas específicas da organização também podem impedir a aplicação automática das configurações STIG, como um requisito para que os administradores revisem as configurações do documento. Para obter mais detalhes sobre quais STIGs são aplicados às AMIs do Windows do Amazon EC2, você pode fazer download de nossa [planilha](#).

Para obter uma lista completa dos STIGs do Windows, consulte a [STIGs Document Library](#). Para obter informações sobre como visualizar a lista completa, consulte [How to View SRGs and STIGs](#) (Como exibir SRGs e STIGs).

- Windows\Baixo

Nenhuma configuração STIG é aplicada ao Microsoft .NET Framework para vulnerabilidades de Categoria III.

- Windows\Médio

V-225238

- Windows\Alto

Nenhuma configuração de STIG adicional é aplicada para vulnerabilidades de Categoria I.

Windows Firewall STIG V1 versão 7

A lista a seguir contém configurações STIG que são aplicadas aos componentes do sistema operacional Windows para AMIs do Amazon EC2 compatíveis com o STIG. Algumas configurações STIG não são aplicadas automaticamente. Isso pode ocorrer devido a limitações técnicas. Por exemplo, a configuração STIG pode não ser aplicável a servidores autônomos. As políticas específicas da organização também podem impedir a aplicação automática das configurações STIG, como um requisito para que os administradores revisem as configurações do documento. Para obter mais detalhes sobre quais STIGs são aplicados às AMIs do Windows do Amazon EC2, você pode fazer download de nossa [planilha](#).

Para obter uma lista completa dos STIGs do Windows, consulte a [STIGs Document Library](#). Para obter informações sobre como visualizar a lista completa, consulte [How to View SRGs and STIGs](#) (Como exibir SRGs e STIGs).

- Windows\Baixo

V-17425, V-17426, V-17427, V-17435, V-17436, V-17437, V-17445, V-17446 e V-17447

- Windows\Médio

V-17415, V-17416, V-17417, V-17419, V-17429 e V-17439

- Windows\Alto

V-17418, V-17428 e V-17438

Internet Explorer (IE) 11 STIG V1 Versão 19

A lista a seguir contém configurações STIG que são aplicadas aos componentes do sistema operacional Windows para AMIs do Amazon EC2 compatíveis com o STIG. Algumas configurações STIG não são aplicadas automaticamente. Isso pode ocorrer devido a limitações técnicas. Por exemplo, a configuração STIG pode não ser aplicável a servidores autônomos. As políticas específicas da organização também podem impedir a aplicação automática das configurações STIG, como um requisito para que os administradores revisem as configurações do documento. Para obter mais detalhes sobre quais STIGs são aplicados às AMIs do Windows do Amazon EC2, você pode fazer download de nossa [planilha](#).

Para obter uma lista completa dos STIGs do Windows, consulte a [STIGs Document Library](#). Para obter informações sobre como visualizar a lista completa, consulte [How to View SRGs and STIGs](#) (Como exibir SRGs e STIGs).

- Windows\Baixo

V-46477, V-46629 e V-97527

- Windows\Médio

V-46473, V-46475, V-46481, V-46483, V-46501, V-46507, V-46509, V-46511, V-46513, V-46515, V-46517, V-46521, V-46523, V-46525, V-46543, V-46545, V-46547, V-46549, V-46553, V-46555, V-46573, V-46575, V-46577, V-46579, V-46581, V-46583, V-46587, V-46589, V-46591, V-46593,

V-46597, V-46599, V-46601, V-46603, V-46605, V-46607, V-46609, V-46615, V-46617, V-46619, V-46621, V-46625, V-46633, V-46635, V-46637, V-46639, V-46641, V-46643, V-46645, V-46647, V-46649, V-46653, V-46663, V-46665, V-46669, V-46681, V-46685, V-46689, V-46691, V-46693, V-46695, V-46701, V-46705, V-46709, V-46711, V-46713, V-46715, V-46717, V-46719, V-46721, V-46723, V-46725, V-46727, V-46729, V-46731, V-46733, V-46779, V-46781, V-46787, V-46789, V-46791, V-46797, V-46799, V-46801, V-46807, V-46811, V-46815, V-46819, V-46829, V-46841, V-46847, V-46849, V-46853, V-46857, V-46859, V-46861, V-46865, V-46869, V-46879, V-46883, V-46885, V-46889, V-46893, V-46895, V-46897, V-46903, V-46907, V-46921, V-46927, V-46939, V-46975, V-46981, V-46987, V-46995, V-46997, V-46999, V-47003, V-47005, V-47009, V-64711, V-64713, V-64715, V-64717, V-64719, V-64721, V-64723, V-64725, V-64729, V-72757, V-72759, V-72761, V-72763, V-75169 e V-75171

- Windows Alto

Nenhuma configuração de STIG adicional é aplicada para vulnerabilidades de Categoria I.

Histórico de versões

A tabela a seguir mostra atualizações de histórico de versão de configurações STIG aplicadas aos sistemas operacionais Windows e componentes do Windows.

Data	AMIs	Detalhes
09/06/2021	Windows Server 2019 STIG V2 R2 Windows Server 2016 STIG V2 R2 Windows Server 2012 R2 STIG V3 R2 Microsoft .NET Framework 4.0 STIG V2 R1 Windows Firewall STIG V1 R7 Internet Explorer 11 STIG V1 R19	Versões atualizadas, quando aplicável, e STIGs aplicados.
5/4/2021	Windows Server 2019 STIG V2 R 1 Windows Server 2016 STIG V2 R 1 Windows Server 2012 R2 STIG V3 R 1 Microsoft .NET Framework 4.0 STIG V2 R 1 Windows Firewall STIG V1 R 7 Internet Explorer 11 STIG V1 R 19	Versões atualizadas, quando aplicável, e STIGs aplicados.
18/9/2020	Windows Server 2019 STIG V1 R 5 Windows Server 2016 STIG V1 R 12 Windows Server 2012 R2 STIG V2 R 19 Internet Explorer 11 STIG V1 R 19 Microsoft .NET Framework 4.0 STIG V1 R 9 Windows Firewall STIG V1 R 7	Versões atualizadas e STIGs aplicados.
6/12/2019	Server 2012 R2 Core e Base V2 R17	Versões atualizadas e STIGs aplicados.

Data	AMIs	Detalhes
	Server 2016 Core e Base V1 R11 Internet Explorer 11 V1 R18 Microsoft .NET Framework 4.0 V1 R9 Windows Firewall STIG V1 R17	
17/9/2019	Server 2012 R2 Core e Base V2 R16 Server 2016 Core e Base V1 R9 Server 2019 Core e Base V1 R2 Internet Explorer 11 V1 R17 Microsoft .NET Framework 4.0 V1 R8	Versão inicial.

AWSHistórico de versões da AMI do Windows da

As tabelas a seguir resumem as alterações para cada versão de AMIs do Windows da AWS. Algumas alterações se aplicam a todas as AMIs do Windows da AWS enquanto outras somente a um subconjunto dessas AMIs.

Tópicos

- [Atualizações mensais de AMI para 2021 \(até o momento\) \(p. 62\)](#)
- [Atualizações mensais de AMI para 2020 \(até o momento\) \(p. 69\)](#)
- [Atualizações mensais de AMI para 2019 \(p. 75\)](#)
- [Atualizações mensais de AMI para 2018 \(p. 80\)](#)
- [Atualizações mensais de AMI para 2017 \(p. 87\)](#)
- [Atualizações mensais de AMI para 2016 \(p. 91\)](#)
- [Atualizações mensais de AMI para 2015 \(p. 95\)](#)
- [Atualizações mensais de AMI para 2014 \(p. 97\)](#)
- [Atualizações mensais de AMI para 2013 \(p. 99\)](#)
- [Atualizações mensais de AMI para 2012 \(p. 101\)](#)
- [Atualizações mensais de AMI para 2011 e anos anteriores \(p. 102\)](#)

Para obter mais informações sobre os componentes incluídos nessas AMIs, consulte o seguinte:

- [Histórico de versões do EC2Launch v](#)
- [Histórico de versões do EC2Launch](#)
- [Histórico de versões do EC2Config \(p. 544\)](#)
- [Notas de release do SSM Agent do Systems Manager](#)
- [Versões do driver do Amazon ENA](#)
- [AWS Drivers PV](#)

Atualizações mensais de AMI para 2021 (até o momento)

Para obter mais informações sobre as atualizações da Microsoft, consulte [Descrição das alterações do conteúdo de serviços de atualização de software e do Windows Server para 2021](#).

Versão	Alterações
2021.09.15	<p>Todas as AMIs</p> <ul style="list-style-type: none">Atualizações de segurança do Windows vigentes em 14 de setembro de 2021AWS Tools for Windows PowerShell versão 3.15.1398SSM versão 3.1.282.0CUs do SQL Server instaladas:<ul style="list-style-type: none">SQL_2019: CU12SQL_2017: CU 25 <p>AMIs Windows Server 2022 e EC2LaunchV2_Preview</p> <ul style="list-style-type: none">EC2Launch v2 versão 2.0.592 <p>AMIs do Windows Server 2012 RTM e R2</p> <ul style="list-style-type: none">EC2Config versão 4.9.4500 <p>As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 12 de maio de 2021 e anteriores se tornaram privadas.</p>
2021.09.01	<p>Novas AMIs do Windows</p> <ul style="list-style-type: none">Windows_Server-2022-English-Full-Base-2021.08.25Windows_Server-2022-English-Full-ContainersLatest-2021.08.25Windows_Server-2022-English-Core-Base-2021.08.25Windows_Server-2022-English-Core-ContainersLatest-2021.08.25Windows_Server-2022-Chinese_Simplified-Full-Base-2021.08.25Windows_Server-2022-Chinese_Traditional-Full-Base-2021.08.25Windows_Server-2022-Czech-Full-Base-2021.08.25Windows_Server-2022-Dutch-Full-Base-2021.08.25Windows_Server-2022-French-Full-Base-2021.08.25Windows_Server-2022-German-Full-Base-2021.08.25Windows_Server-2022-Hungarian-Full-Base-2021.08.25Windows_Server-2022-Italian-Full-Base-2021.08.25Windows_Server-2022-Japanese-Full-Base-2021.08.25Windows_Server-2022-Korean-Full-Base-2021.08.25Windows_Server-2022-Polish-Full-Base-2021.08.25Windows_Server-2022-Portuguese_Brazil-Full-Base-2021.08.25Windows_Server-2022-Portuguese_Portugal-Full-Base-2021.08.25Windows_Server-2022-Russian-Full-Base-2021.08.25Windows_Server-2022-Spanish-Full-Base-2021.08.25Windows_Server-2022-Swedish-Full-Base-2021.08.25Windows_Server-2022-Turkish-Full-Base-2021.08.25 <p>As AMIs do Windows Server 2022 incluem o EC2Launch v2 por padrão. Para obter mais informações, consulte Visão geral do EC2Launch v2 (p. 483).</p>

Versão	Alterações
	<p>AMIs EC2LaunchV2_Preview</p> <ul style="list-style-type: none"> EC2Launch v2 versão 2.0.592
2021.08.11	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança do Windows vigentes em 10 de agosto de 2021 AWS Tools for Windows PowerShell versão 3.15.13571 EC2Launch versão 1.3.2003411 SSM versão 3.0.1181.0 CUs do SQL Server instaladas: <ul style="list-style-type: none"> SQL_2019: CU11 <p>AMIs EC2LaunchV2_Preview</p> <ul style="list-style-type: none"> EC2Launch v2 versão 2.0.548 <p>As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 14 de abril de 2021 e anteriores se tornaram privadas.</p>
2021.07.14	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança do Windows vigentes em 13 de julho de 2021 AWS Tools for Windows PowerShell versão 3.15.1350 EC2Launch version 1.3.2003364 CUs do SQL Server instaladas: <ul style="list-style-type: none"> SQL_2017: CU24
2021.07.07	<p>Todas as AMIs</p> <p>Versão da AMI fora de banda que aplica a atualização de segurança fora de banda de julho lançada recentemente pela Microsoft como mitigação adicional para CVE-34527.</p> <p>Note</p> <p>O <code>HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint</code> não está definido nas AMIs do Windows fornecidas pela AWS, que é o estado padrão.</p> <p>Para obter mais informações, consulte:</p> <ul style="list-style-type: none"> https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527 https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7 <p>As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 10 de março de 2021 e anteriores se tornaram privadas.</p>

Versão	Alterações
2021.06.09	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 8 de junho de 2021• AWS Tools for Windows PowerShell versão 3.15.1326• SSM version 3.0.1124.0 <p>AMIs do Windows Server 2012RTM/2012 R2</p> <ul style="list-style-type: none">• EC2Config version 4.9.4419
2021.05.12	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 11 de maio de 2021• AWS Tools for Windows PowerShell versão 3.15.1302• EC2Launch versão 1.3.2003312• CUs do SQL Server instaladas:<ul style="list-style-type: none">• SQL_2019: CU10• As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 10 de fevereiro de 2021 e anteriores se tornaram privadas. <p>AMIs do Windows Server 2012RTM/2012 R2</p> <ul style="list-style-type: none">• EC2Config versão 4.9.4381• SSM versão 3.0.529.0 <p>AMIs com GPU NVIDIA</p> <ul style="list-style-type: none">• GRID versão 462.31• Tesla versão 462.31 <p>AMIs com GPU Radeon</p> <ul style="list-style-type: none">• Radeon versão 20.10.25.04

Versão	Alterações
14/04/2021	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 13 de abril de 2021• AWS Tools for Windows PowerShell versão 3.15.1280• AWS PV versão 8.4.0• cfn-init versão 2.0.6. Este pacote inclui o Microsoft Visual C++ 2015-2019 Versão 14.28.29913.0 redistribuível como uma dependência.• AWS ENA versão 2.2.3• EC2Launch versão 1.3.2003284• CUs do SQL Server instaladas:<ul style="list-style-type: none">• SQL_2017: CU23• As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 13 de janeiro de 2021 e anteriores se tornaram privadas.• Note<p>O Windows Server 1909 chega ao fim do suporte em 11 de maio de 2021. Todas as versões públicas das imagens a seguir se tornarão privadas no dia 11 de maio de 2021. Instâncias existentes e imagens personalizadas pertencentes à sua conta baseadas no Windows Server 1909 não serão afetadas. Para manter o acesso ao Windows Server 1909, crie uma imagem personalizada na sua conta antes de 11 de maio de 2021.</p><ul style="list-style-type: none">• Windows_Server-1909-English-Core-Base• Windows_Server-1909-English-Core-ContainersLatest <p>AMIs EC2LaunchV2_Preview</p> <ul style="list-style-type: none">• EC2Launch v2 versão 2.0.285

Versão	Alterações
11.03.2021	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 9 de março de 2021• AWS Tools for Windows PowerShell versão 3.15.1248• cfn-init versão 2.0.5 Este pacote inclui Microsoft Visual C++ 2015-2019 Versão 14.28.29910.0 redistribuível como uma dependência.• EC2Launch versão 1.3.2003236• SSM Agent versão 3.0.529.0• NVIDIA GRID versão 461.33• CUs do SQL Server instaladas:<ul style="list-style-type: none">• SQL 2016_SP2: CU16• SQL 2019: CU9• Atualização KB4577586 para a remoção do Adobe Flash Player instalado em todas as imagens aplicáveis (o Adobe Flash Player não está habilitado por padrão em todas as imagens). <p>Note</p> <p>As CAs raiz da Amazon foram adicionadas ao repositório de certificados das Autoridades de certificação raiz confiáveis em todas as AMIs. Para obter mais informações, consulte https://www.amazontrust.com/repository/#rootcas.</p> <p>AMIs do Windows Server 2016 e 2019</p> <ul style="list-style-type: none">• Atualizado das versões padrão do framework .NET para a versão 4.8. <p>AMIs do Windows Server 2012RTM/2012 R2</p> <ul style="list-style-type: none">• EC2Config versão 4.9.4326• SSM Agent versão 3.0.431.0

Versão	Alterações
2021.02.10	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows atuais para 9 de fevereiro de 2021• AWS Tools for Windows PowerShell versão 3.15.1224• NVIDIA GRID versão 461.09 <p>Desde março de 2021, as AMIs do Windows provisionadas pela AWS incluem as CAs raiz da Amazon no armazenamento de certificados para minimizar possíveis interrupções da próxima migração de certificados do S3 e do CloudFront, que estava programada para 23 de março de 2021. Para obter mais informações, consulte:</p> <ul style="list-style-type: none">• https://aws.amazon.com/blogs/security/how-to-prepare-for-aws-move-to-its-own-certificate-authority/• https://forums.aws.amazon.com/ann.jspa?annID=7541 <p>Além disso, a AWS aplicará a “Atualização para a remoção do Adobe Flash Player” (KB4577586) a todas as AMIs do Windows em março para remover o Adobe Flash Player integrado, cujo suporte encerrou em 31 de dezembro de 2020. Se o seu caso de uso exigir o Adobe Flash Player integrado, recomendamos criar uma imagem personalizada baseada em AMIs com a versão 2021.02.10 ou anterior. Para obter mais informações sobre o fim do suporte do Adobe Flash Player, consulte:</p> <ul style="list-style-type: none">• https://blogs.windows.com/msedge/2020/09/04/update-adobe-flash-end-support/• https://www.adobe.com/products/flashplayer/end-of-life.html <p>AMIs EC2LaunchV2_Preview</p> <ul style="list-style-type: none">• EC2Launch v2 versão 2.0.207 <p>Novas AMIs do Windows</p> <ul style="list-style-type: none">• Windows_Server-2016-Japanese-Full-SQL_2019_Enterprise-2021.02.10• Windows_Server-2016-Japanese-Full-SQL_2019_Standard-2021.02.10• Windows_Server-2016-Japanese-Full-SQL_2019_Web-2021.02.10• Windows_Server-2019-Japanese-Full-SQL_2019_Enterprise-2021.02.10• Windows_Server-2019-Japanese-Full-SQL_2019_Standard-2021.02.10• Windows_Server-2019-Japanese-Full-SQL_2019_Web-2021.02.10

Versão	Alterações
2021.01.13	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 12 de janeiro de 2021• AWS Tools for Windows PowerShell versão 3.15.1204• AWS ENA versão 2.2.2• EC2Launch v1 versão 1.3.2003210 <p>AMIs do Windows Server SAC/2019/2016</p> <ul style="list-style-type: none">• SSM Agent versão 3.0.431.0

Atualizações mensais de AMI para 2020 (até o momento)

Para obter mais informações sobre as atualizações da Microsoft, consulte [Descrição das alterações do conteúdo de serviços de atualização de software e do Windows Server para 2020](#).

Versão	Alterações
2020.12.09	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 8 de dezembro de 2020• AWS Tools for Windows PowerShell versão 3.15.1181• Todas as AMIs do SQL Server Enterprise, Standard e Web agora incluem mídia de instalação do SQL Server em C:\SQLServerSetup• EC2Launch v1 versão 1.3.2003189• As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 9 de setembro de 2020 e anteriores se tornaram privadas. <p>AMIs do Windows Server 2012/2012 R2</p> <ul style="list-style-type: none">• EC2Config versão 4.9.4279• SSM Agent versão 2.3.871.0 <p>AMIs EC2LaunchV2_Preview</p> <ul style="list-style-type: none">• EC2Launch v2 versão 2.0.160
2020.11.11	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 10 de novembro de 2020• AWS Tools for Windows PowerShell versão 3.15.1160• CUs do SQL Server instaladas:<ul style="list-style-type: none">• SQL 2016 SP2: CU15• SQL 2017: CU22• SQL 2019: CU8• SSM Agent versão 2.3.1644.0• AMIs de visualização do EC2Launch v2: EC2Launch versão 2.0.153

Versão	Alterações
	<ul style="list-style-type: none">As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 12 de agosto de 2020 e anteriores se tornaram privadas. <p>Novas AMIs do Windows</p> <ul style="list-style-type: none">Windows_Server-20H2-Inglês-Core Base-2020.11.11Windows_Server-20H2-Inglês Core-Containerslatest-2020.11.11
14.10.2020	<p>Todas as AMIs</p> <ul style="list-style-type: none">Atualizações de segurança do Windows vigentes em 13 de outubro de 2020AWS Tools for Windows PowerShell versão 3.15.1140NVIDIA GRID versão 452.39AMIs de visualização do EC2Launch v2: EC2Launch versão 2.0.146AWS ENA versão 2.2.1cfn-init versão 1.4.34As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 15 de julho de 2020 e anteriores se tornaram privadas.
25.9.2020	<p>Uma nova versão de imagens de máquina da Amazon com o SQL Server 2019 datada de 25.9.2020 foi lançada. Essa versão inclui os mesmos componentes de software que a versão anterior datada de 09.09.2020, mas não inclui o CU7 para SQL 2019, que foi recentemente removido da disponibilidade pública pela Microsoft devido a um problema conhecido com a confiabilidade do recurso de snapshot do banco de dados. Para obter mais informações, consulte a seguinte publicação do blog da Microsoft: https://techcommunity.microsoft.com/t5/sql-server/cumulative-update-7-for-sql-server-2019-rtm-removed/ba-p/1629317.</p> <p>Novas AMIs do Windows</p> <ul style="list-style-type: none">Windows_Server-2016-English-Full-SQL_2019_Enterprise-2020.09.25Windows_Server-2016-English-Full-SQL_2019_Express-2020.09.25Windows_Server-2016-English-Full-SQL_2019_Standard-2020.09.25Windows_Server-2016-English-Full-SQL_2019_Web-2020.09.25Windows_Server-2019-English-Full-SQL_2019_Enterprise-2020.09.25Windows_Server-2019-English-Full-SQL_2019_Express-2020.09.25Windows_Server-2019-English-Full-SQL_2019_Standard-2020.09.25Windows_Server-2019-English-Full-SQL_2019_Web-2020.09.25 <p>AMIs EC2LaunchV2_Preview</p> <ul style="list-style-type: none">EC2LaunchV2_Preview-Windows_Server-2019-English-Full-SQL_2019_Express-2020.09.25

Versão	Alterações
2020.9.9	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 8 de setembro de 2020• AWSDrivers PV versão 8.3.4• AWS ENA versão 2.2.0• AWS Tools for Windows PowerShell versão 3.15.1110• CUs do SQL Server instaladas<ul style="list-style-type: none">• SQL_2016_SP2: CU14• SQL_2019: CU7• As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 10 de junho de 2020 e anteriores se tornaram privadas. <p>AMIs do Windows Server 2016/2019/1809/1903/1909/2004</p> <ul style="list-style-type: none">• EC2Launch versão 1.3.2003155• SSM Agent versão 2.3.1319.0 <p>AMIs EC2LaunchV2_Preview</p> <ul style="list-style-type: none">• EC2Launch v2 versão 2.0.124
2020.8.12	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 11 de agosto de 2020• AWS Tools for Windows PowerShell versão 3.15.1084• AMIs G3: NVIDIA GRID versão 451.48• AMIs de visualização do EC2Launch v2: EC2Launch versão 2.0.104• CUs do SQL instaladas:<ul style="list-style-type: none">• SQL_2019: CU6• As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 13 de maio de 2020 e anteriores se tornaram privadas.
2020.7.15	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 14 de julho de 2020.• AWS Tools for Windows PowerShell versão 3.15.1064• ENA versão 2.1.5• CUs do SQL Server instaladas<ul style="list-style-type: none">• SQL_2017: CU21• SQL_2019: CU5• As versões anteriores das AMIs do Windows publicadas pela Amazon datadas de 15 de abril de 2020 e anteriores se tornaram privadas.

Versão	Alterações
01.7.2020	<p>Uma nova versão das Imagens de máquina da Amazon foi lançada. Essas imagens incluem o EC2Launch v2 e servem como visualização funcional do novo agente de execução antes de ser incluído por padrão em todas as AMIs do Windows atualmente fornecidas pela AWS no final deste ano. Observe que alguns documentos do SSM e serviços dependentes, como o EC2 Image Builder, podem exigir atualizações para oferecer suporte ao EC2 Launch v2. Essas atualizações ocorrerão nas próximas semanas. Essas imagens não são recomendadas para uso em ambientes de produção. Leia mais sobre o EC2Launch v2 em https://aws.amazon.com/about-aws/whats-new/2020/07/introducing-ec2-launch-v2-simplify-customizing-windows-instances/ e Configurar uma instância do Windows usando o EC2Launch v2 (p. 482). Todas as AMIs atuais do Windows Server continuarão a ser fornecidas sem alterações ao agente de execução atual, seja EC2Config (Server 2012 RTM ou 2012 R2) ou EC2Launch v1 (Server 2016 ou posterior), nos próximos meses. Num futuro próximo, todas as AMIs do Windows Server atualmente fornecidas pela AWS serão migradas para usar o EC2Launch v2 por padrão como parte do release mensal. As AMIs do EC2LaunchV2_Preview serão atualizadas mensalmente e permanecerão disponíveis até que essa migração ocorra.</p> <p>Novas AMIs do Windows</p> <ul style="list-style-type: none"> • EC2LaunchV2_Preview-Windows_Server-2004-English-Core-Base-2020.06.30 • EC2LaunchV2_Preview-Windows_Server-2019-English-Full-Base-2020.06.30 • EC2LaunchV2_Preview-Windows_Server-2019-English-Core-Base-2020.06.30 • EC2LaunchV2_Preview-Windows_Server-2016-English-Full-Base-2020.06.30 • EC2LaunchV2_Preview-Windows_Server-2016-English-Core-Base-2020.06.30 • EC2LaunchV2_Preview-Windows_Server-2012_R2_RTM-English-Full-Base-2020.06.30 • EC2LaunchV2_Preview-Windows_Server-2012_R2_RTM-English-Core-Base-2020.06.30 • EC2LaunchV2_Preview-Windows_Server-2012_RTM-English-Full-Base-2020.06.30 • EC2LaunchV2_Preview-Windows_Server-2019-English-Full-SQL_2019_Express-2020.06.30 • EC2LaunchV2_Preview-Windows_Server-2016-English-Full-SQL_2017_Express-2020.06.30
2020.6.10	<p>Todas as AMIs</p> <ul style="list-style-type: none"> • Atualizações de segurança do Windows vigentes em 9 de junho de 2020. • AWS Tools for Windows PowerShell versão 3.15.1034 • cfn-init versão 1.4.33 • SQL CU instalado: SQL_2016_SP2: CU13
27/5/2020	<p>Novas AMIs do Windows</p> <ul style="list-style-type: none"> • Windows_Server-2004-English-Core-Base-2020.05.27 • Windows_Server-2004-English-Core-ContainersLatest-2020.05.27

Versão	Alterações
2020.5.13	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 12 de maio de 2020• AWS Tools for Windows PowerShell versão 3.15.1013• EC2Launch versão 1.3.2003150
2020.4.15	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 14 de abril de 2020• AWS Tools for Windows PowerShell versão 3.15.998• EC2Config versão 4.9.4222• EC2Launch versão 1.3.2003040• SSM Agent versão 2.3.842.0• CUs do SQL Server instaladas:<ul style="list-style-type: none">• SQL_2017: CU 20• SQL_2019: CU 4
2020.3.18	<p>AMIs do Windows Server</p> <p>Resolve um problema intermitente descoberto na versão 2020.3.11 em que o Background Intelligent Transfer Service (BITS) pode não iniciar dentro do período esperado após a inicialização inicial do sistema operacional, podendo resultar em tempos limite, erros BITS no log de eventos ou falhas de cmdlets envolvendo BITS invocados rapidamente após a inicialização inicial. Outras AMIs do Windows Server não são afetadas por esse problema e sua versão mais recente permanece 2020.03.11.</p>
2020.3.11	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows vigentes em 10 de março de 2020• AWS Tools for Windows PowerShell versão 3.15.969• EC2Config versão 4.9.4122• EC2Launch versão 1.3.2002730• SSM Agent versão 2.3.814.0• CUs do SQL Server instaladas:<ul style="list-style-type: none">• SQL_2016_SP2: CU 12• SQL_2017: CU 19• SQL_2019: CU 2 não aplicado devido a um problema conhecido no SQL Agent• Atualização de segurança fora de banda (KB4551762) para o núcleo do servidor 1909 e 1903 aplicada para mitigar o CVE-2020-0796. Outras versões do Windows Server não são afetadas por esse problema. Para obter mais detalhes, consulte https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

Versão	Alterações
2020.2.12	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança do Windows atuais para 11 de fevereiro de 2020• AWS Tools for Windows PowerShell versão 3.15.945• Atualizações de driver Intel SRIOV<ul style="list-style-type: none">• 2019/1903/1909: versão 2.1.185.0• 2016/1809: versão 2.1.186.0• 2012 R2: versão 1.2.199.0• CUs do SQL Server instaladas:<ul style="list-style-type: none">• SQL_2019: CU 1• SQL_2017: CU 18• SQL_2016_SP2: CU 11 <p>Microsoft Windows Server 2008 SP2 e Windows Server 2008 R2</p> <p>O Windows Server 2008 SP2 e o Windows Server 2008 R2 alcançaram o encerramento do suporte (EOS) em 14/1/2020 e já não receberão atualizações de segurança regulares da Microsoft. A AWS deixará de publicar ou distribuir AMIs do Windows Server 2008 SP2 ou Windows Server 2008 R2. As instâncias existentes do 2008 SP2/R2 e AMIs personalizadas na sua conta não serão afetadas e você pode continuar a usá-las após a data de encerramento do suporte.</p> <p>Para obter mais informações sobre o encerramento do suporte da Microsoft na AWS, incluindo as opções de atualização e importação, além de uma lista completa de AMIs que não serão mais publicadas a partir de 14/01/2020, consulte End of Support (EOS) for Microsoft Products (Encerramento do suporte (EOS) para produtos Microsoft).</p>
2020.1.15	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em janeiro de 14 de 2020• AWS Tools for Windows PowerShell versão 3.15.925• ENA versão 2.1.4 <p>Microsoft Windows Server 2008 SP2 e Windows Server 2008 R2</p> <p>O Windows Server 2008 SP2 e o Windows Server 2008 R2 alcançaram o encerramento do suporte (EOS) em 14/1/2020 e já não receberão atualizações de segurança regulares da Microsoft. A AWS deixará de publicar ou distribuir AMIs do Windows Server 2008 SP2 ou Windows Server 2008 R2. As instâncias existentes do 2008 SP2/R2 e AMIs personalizadas na sua conta não serão afetadas e você pode continuar a usá-las após a data de encerramento do suporte.</p> <p>Para obter mais informações sobre o encerramento do suporte da Microsoft na AWS, incluindo as opções de atualização e importação, além de uma lista completa de AMIs que não serão mais publicadas a partir de 14/01/2020, consulte End of Support (EOS) for Microsoft Products (Encerramento do suporte (EOS) para produtos Microsoft).</p>

Atualizações mensais de AMI para 2019

Para obter mais informações sobre as atualizações da Microsoft, consulte [Descrição das alterações do conteúdo de serviços de atualização de software e do Windows Server para 2019](#).

Versão	Alterações
16/12/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 10 de dezembro de 2019• AWS Tools for Windows PowerShell versão 3.15.903 <p>Microsoft Windows Server 2008 SP2 e Windows Server 2008 R2</p> <p>A Microsoft encerrará o suporte mainstream para o Windows Server 2008 SP2 e Windows Server 2008 R2 em 14 de janeiro de 2020. Nessa data, a AWS não publicará mais ou distribuirá AMIs do Windows Server 2008 SP2 ou do Windows Server 2008 R2. Instâncias existentes do 2008 SP2/R2 e AMIs personalizadas na sua conta não serão afetadas e você pode continuar a usá-las após a data de encerramento do suporte (EOS).</p> <p>Para obter mais informações sobre o Microsoft EOS na AWS, incluindo opções de atualização e importação, juntamente com uma lista completa de AMIs que não serão mais publicadas ou distribuídas em 14 de janeiro de 2020, consulte End of Support (EOS) for Microsoft Products (Encerramento do suporte (EOS) para produtos Microsoft).</p>
13/11/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• AWS Tools for Windows PowerShell versão 3.15.876• As atualizações de segurança do Windows atuais são de 12 de novembro de 2019• EC2 Config versão 4.9.3865• EC2 Launch versão 1.3.2002240• SSM Agent v2.3.722.0 <p>Versões anteriores de AMIs foram marcadas como privadas.</p> <p>Novas AMIs do Windows</p> <ul style="list-style-type: none">• Windows_Server-1909-English-Core-Base-2019.11.13• Windows_Server-1909-English-Core-ContainersLatest-2019.11.13• Windows_Server-2016-English-Full-SQL_2019_Enterprise-2019.11.13• Windows_Server-2016-English-Full-SQL_2019_Express-2019.11.13• Windows_Server-2016-English-Full-SQL_2019_Standard-2019.11.13• Windows_Server-2016-English-Full-SQL_2019_Web-2019.11.13• Windows_Server-2019-English-Full-SQL_2019_Enterprise-2019.11.13• Windows_Server-2019-English-Full-SQL_2019_Express-2019.11.13• Windows_Server-2019-English-Full-SQL_2019_Standard-2019.11.13• Windows_Server-2019-English-Full-SQL_2019_Web-2019.11.13

Versão	Alterações
05/11/2019	<p>Novas AMIs do Windows</p> <p>Novas AMIs do SQL disponíveis:</p> <ul style="list-style-type: none">• Windows_Server-2016-English-Full-SQL_2019_Enterprise-2019.11.05• Windows_Server-2016-English-Full-SQL_2019_Express-2019.11.05• Windows_Server-2016-English-Full-SQL_2019_Standard-2019.11.05• Windows_Server-2016-English-Full-SQL_2019_Web-2019.11.05• Windows_Server-2019-English-Full-SQL_2019_Enterprise-2019.11.05• Windows_Server-2019-English-Full-SQL_2019_Express-2019.11.05• Windows_Server-2019-English-Full-SQL_2019_Standard-2019.11.05• Windows_Server-2019-English-Full-SQL_2019_Web-2019.11.05
09.10.2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• AWS Tools for Windows PowerShell versão 3.15.846• Atualizações de segurança do Windows vigentes em 8 de outubro de 2019• Atualizações da plataforma Windows Defender vigente e bloqueio de atualização através de registro removido. Para obter mais detalhes, consulte https://support.microsoft.com/en-us/help/4513240/sfc-incorrectly-flags-windows-defender-ps-files-as-corrupted <p>Novas AMIs do Windows</p> <p>Nova AMI otimizada para ECS:</p> <ul style="list-style-type: none">• Windows_Server-2019-English-Core-ECS_Optimized-2019.10.09
12/09/2019	<p>Nova AMI do Windows</p> <ul style="list-style-type: none">• amzn2-ami-hvm-2.0.20190618-x86_64-gp2-mono <p>.NET Core 2.2, Mono 5.18, e PowerShell 6.2 pré-instalados para executar suas aplicações .NET no Amazon Linux 2 com suporte em longo prazo (LTS, Long Term Support)</p>

Versão	Alterações
11/09/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• AWSDriver PV versão 8.3.2• AWSDriver NVMe versão 1.3.2• AWS Tools for Windows PowerShell versão 3.15.826• NLA ativado em todos os sistemas operacionais 2012 RTM para AMIs 2019• Driver Intel 82599 VF voltou para a versão 2.0.210.0 (Server 2016) ou versão 2.1.138.0 (Server 2019) devido a problemas relatados por clientes. Interação com a Intel a respeito desses problemas contínuos.• Atualizações de segurança do Windows vigentes em 10 de setembro de 2019• Bloqueio da atualização da plataforma do Windows Defender por registro devido a falhas de SFC introduzidas pelo cliente mais recente. Será ativada novamente quando houver patch disponível. Consulte https://support.microsoft.com/en-us/help/4513240/sfc-incorrectly-flags-windows-defender-ps-files-as-corrupted. Bloqueio de atualização de plataforma: HKLM:\SOFTWARE\Microsoft\Windows Defender\Miscellaneous Configuration\PreventPlatformUpdate type=DWORD, value=1 <p>Versões anteriores de AMIs foram marcadas como privadas.</p> <p>Novas AMIs do Windows</p> <p>Novas AMIs disponíveis em conformidade com STIG:</p> <ul style="list-style-type: none">• Windows_Server-2012-R2-English-STIG-Full• Windows_Server-2012-R2-English-STIG-Core• Windows_Server-2016-English-STIG-Full• Windows_Server-2016-English-STIG-Core• Windows_Server-2019-English-STIG-Full• Windows_Server-2019-English-STIG-Core <p>Windows Server 2008 R2 SP1</p> <p>Inclui as seguintes atualizações, que são necessárias para atualizações ESU (Microsoft Extended Security).</p> <ul style="list-style-type: none">• KB4490628• KB4474419• KB4516655 <p>Windows Server 2008 SP2</p> <p>Inclui as seguintes atualizações, que são necessárias para atualizações ESU (Microsoft Extended Security).</p> <ul style="list-style-type: none">• KB4493730• KB4474419• KB4517134

Versão	Alterações
	<p>Note</p> <p>A NLA agora está habilitada em todas as AMIs 2012 RTM, 2012 R2 e 2016 para aumentar a postura de segurança padrão de RDP. A NLA permanece habilitada nas AMIs de 2019.</p>
16/ago/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 13 de agosto de 2019. Inclui KBs que abordam CVE-2019-1181, CVE-2019-1182, CVE-2019-1222 e CVE-2019-1226. EC2Config versão 4.9.3519 SSM Agent versão 2.3.634.0 AWS Tools for Windows PowerShell versão 3.15.802 Bloqueio da atualização da plataforma do Windows Defender por registro devido a falhas de SFC introduzidas pela atualização. A atualização será habilitada novamente quando um novo patch estiver disponível. <p>Note</p> <p>A partir de setembro, a NLA será habilitada em todas as AMIs 2012 RTM, 2012 R2 e 2016 para aumentar a postura de segurança padrão de RDP</p>
19/07/2019	<p>Novas AMIs do Windows</p> <ul style="list-style-type: none"> Windows_Server-2016-English-Full-ECS_Optimized-2019.07.19 Windows_Server-2019-English-Full-ECS_Optimized-2019.07.19
12/07/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 9 de julho de 2019
2019.06.12	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 11 de junho de 2019 AWS SDK versão 3.15.756 AWSDriver PV versão 8.2.7 AWSDriver NVMe versão 1.3.1 As AMIs "P3" a seguir mudarão de nome para AMIs "Tesla". Essas AMIs serão compatíveis com todas as instâncias da AWS compatíveis com GPU usando o driver Tesla. As AMIs P3 não serão mais atualizadas depois desta versão e serão removidas como parte do nosso ciclo regular. <ul style="list-style-type: none"> Windows_Server-2012-R2_RTM-English-P3-2019.06.12 substituído por Windows_Server-2012-R2_RTM-English-Tesla-2019.06.12 Windows_Server-2016-English-P3-2016.06.12 substituído por Windows_Server-2016-English-Tesla-2019.06.12 <p>Novas AMIs do Windows</p> <ul style="list-style-type: none"> Windows_Server-2019-English-Tesla-2019.06.12 <p>Versões anteriores de AMIs foram marcadas como privadas.</p>

Versão	Alterações
21/05/2019	<p>Windows Server, versão 1903</p> <ul style="list-style-type: none">• Agora, as AMIs estão disponíveis
15.05.2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 14 de maio de 2019• EC2Config versão 4.9.3429• SSM Agent versão 2.3.542.0• AWS SDK versão 3.15.735
26/04/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Corrigidas AMIs do Windows Server 2019 com SQL para tratar casos de presença onde a primeira inicialização de uma instância pode resultar em impedimento de instância e o Windows exibe a mensagem "Aguarde o serviço de perfil de usuário".
21/04/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• AWSReversão da versão 8.2.6 do driver PV para a versão 8.3.0
10/04/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 9 de abril de 2019• AWS SDK versão 3.15.715• AWSDriver PV versão 8.3.0• EC2Launch versão 1.3.2001360 <p>Novas AMIs do Windows</p> <ul style="list-style-type: none">• Windows_Server-2016-English-Full-SQL_2012_SP4_Standard-2019.04.10• Windows_Server-2016-English-Full-SQL_2014_SP3_Standard-2019.04.10• Windows_Server-2016-English-Full-SQL_2014_SP3_Enterprise-2019.04.10
13/03/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 12 de março de 2019• AWS SDK versão 3.15.693• EC2Launch versão 1.3.2001220• Driver NVIDIA Tesla versão 412.29 para deep learning e AMIs de P3 (https://nvidia.custhelp.com/app/answers/detail/a_id/4772) <p>Versões anteriores de AMIs foram marcadas como privadas</p>

Versão	Alterações
13/02/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 12 de fevereiro de 2019• SSM Agent versão 2.3.444.0• AWS SDK versão 3.15.666• EC2Launch versão 1.3.2001040• EC2Config versão 4.9.3289• AWSDriver PV 8.2.6• Ferramenta NVMe do EBS <p>O SQL 2014 com Service Pack 2 e o SQL 2016 com Service Pack 1 não serão mais atualizados após essa versão.</p>
09/02/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• As AMIs do Windows foram atualizadas. Novas AMIs podem ser encontradas nas seguintes versões de data: <p>Novembro, "29.11.2018"</p> <p>Dezembro, "13.12.2018"</p> <p>Janeiro, "09.02.2019"</p> <p>Versões anteriores de AMIs foram marcadas como privadas</p>
10/01/2019	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 10 de janeiro de 2019• SSM Agent versão 2.3.344.0• AWS SDK versão 3.15.647• EC2Launch versão 1.3.2000930• EC2Config versão 4.9.3160 <p>Todas as AMIs com SQL Server</p> <ul style="list-style-type: none">• Últimas atualizações cumulativas

Atualizações mensais de AMI para 2018

Para obter mais informações sobre as atualizações da Microsoft, consulte [Descrição das alterações do conteúdo de serviços de atualização de software e do Windows Server para 2018](#).

Versão	Alterações
2018.12.12	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 12 de dezembro de 2018• SSM Agent versão 2.3.274.0• AWS SDK versão 3.15.629

Versão	Alterações
	<ul style="list-style-type: none">• EC2Launch versão 1.3.2000760 <p>Novas AMIs do Windows</p> <ul style="list-style-type: none">• Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2014_SP3_Standard-2018.12.12• Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2014_SP3_Express-2018.12.12• Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP3_Enterprise-2018.12.12• Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP3_Standard-2018.12.12• Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP3_Express-2018.12.12• Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP3_Web-2018.12.12• Windows_Server-2012-RTM-Japanese-64Bit-SQL_2014_SP3_Express-2018.12.12• Windows_Server-2012-RTM-Japanese-64Bit-SQL_2014_SP3_Standard-2018.12.12• Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP3_Express-2018.12.12• Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP3_Web-2018.12.12• Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2_Web-2018.12.12• Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2_Express-2018.12.12• Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Enterprise-2018.12.12• Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Standard-2018.12.12• Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Express-2018.12.12• Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP2_Web-2018.12.12• Windows_Server-2012-R2_RTM-Japanese-64Bit-SQL_2016_SP2_Standard-2018.12.12• Windows_Server-2016-Korean-Full-SQL_2016_SP2_Standard-2018.12.12• Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Enterprise-2018.12.12• Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Web-2018.12.12• Windows_Server-2016-English-Full-SQL_2016_SP2_Web-2018.12.12• Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Standard-2018.12.12• Windows_Server-2016-English-Full-SQL_2016_SP2_Express-2018.12.12• Windows_Server-2016-English-Full-SQL_2016_SP2_Standard-2018.12.12• Windows_Server-2016-English-Core-SQL_2016_SP2_Enterprise-2018.12.12• Windows_Server-2016-English-Core-SQL_2016_SP2_Web-2018.12.12• Windows_Server-2016-English-Core-SQL_2016_SP2_Express-2018.12.12• Windows_Server-2016-English-Core-SQL_2016_SP2_Standard-2018.12.12

Versão	Alterações
	<ul style="list-style-type: none"> • Windows_Server-2016-Japanese-Full-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2016-Korean-Full-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2019-Spanish-Full-Base-2018.12.12 • Windows_Server-2019-Japanese-Full-Base-2018.12.12 • Windows_Server-2019-Portuguese_Portugal-Full-Base-2018.12.12 • Windows_Server-2019-Chinese_Traditional-Full-Base-2018.12.12 • Windows_Server-2019-Italian-Full-Base-2018.12.12 • Windows_Server-2019-Swedish-Full-Base-2018.12.12 • Windows_Server-2019-English-Core-Base-2018.12.12 • Windows_Server-2019-Hungarian-Full-Base-2018.12.12 • Windows_Server-2019-Polish-Full-Base-2018.12.12 • Windows_Server-2019-Turkish-Full-Base-2018.12.12 • Windows_Server-2019-Korean-Full-Base-2018.12.12 • Windows_Server-2019-Dutch-Full-Base-2018.12.12 • Windows_Server-2019-German-Full-Base-2018.12.12 • Windows_Server-2019-Russian-Full-Base-2018.12.12 • Windows_Server-2019-Czech-Full-Base-2018.12.12 • Windows_Server-2019-English-Full-Base-2018.12.12 • Windows_Server-2019-French-Full-Base-2018.12.12 • Windows_Server-2019-Portuguese_Brazil-Full-Base-2018.12.12 • Windows_Server-2019-Chinese_Simplified-Full-Base-2018.12.12 • Windows_Server-2019-English-Full-HyperV-2018.12.12 • Windows_Server-2019-English-Full-ContainersLatest-2018.12.12 • Windows_Server-2019-English-Core-ContainersLatest-2018.12.12 • Windows_Server-2019-English-Full-SQL_2017_Enterprise-2018.12.12 • Windows_Server-2019-English-Full-SQL_2017_Standard-2018.12.12 • Windows_Server-2019-English-Full-SQL_2017_Web-2018.12.12 • Windows_Server-2019-English-Full-SQL_2017_Express-2018.12.12 • Windows_Server-2019-English-Full-SQL_2016_SP2_Enterprise-2018.12.12 • Windows_Server-2019-English-Full-SQL_2016_SP2_Standard-2018.12.12 • Windows_Server-2019-English-Full-SQL_2016_SP2_Web-2018.12.12 • Windows_Server-2019-English-Full-SQL_2016_SP2_Express-2018.12.12 <p style="text-align: center;">AMI do Linux atualizada</p> <ul style="list-style-type: none"> • amzn2-ami-hvm-2.0.20180622.1-x86_64-gp2-dotnetcore-2018.12.12
28/11/2018	<p>Todas as AMIs</p> <ul style="list-style-type: none"> • SSM Agent versão 2.3.235.0 • Alterações em todos os esquemas de alimentação para definir o vídeo para nunca desligar

Versão	Alterações
20/11/2018	<p>Windows_Server-2016-English-Deep-Learning</p> <p>Windows_Server-2016-English-Deep-Learning</p> <ul style="list-style-type: none">TensorFlow versão 1.12MXNet versão 1.3NVIDIA versão 392.05
19/11/2018	<p>Todas as AMIs</p> <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em 19 de novembro de 2018AWS SDK versão 3.15.602.0SSM Agent versão 2.3.193.0EC2Config versão 4.9.3067Configurações INF do Chipset Intel para oferecer suporte a novos tipos de instância <p>Windows Server versão 1809</p> <ul style="list-style-type: none">Agora, as AMIs estão disponíveis.
2018.10.14	<p>Todas as AMIs</p> <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em 9 de outubro de 2018AWS Tools for Windows PowerShell versão 3.3.365.0CloudFormation versão 1.4.31AWSDriver PV versão 8.2.4AWS PCI Serial Driver versão 1.0.0.0 (suporte para Windows 2008R2 e 2012 em instâncias Bare Metal)ENA Driver versão 1.5.0 <p>Microsoft Windows Server 2016 Datacenter e Standard Editions para Nano Server</p> <p>A Microsoft encerrou o suporte mainstream para as opções de instalação do Windows Server 2016 Datacenter e Standard Editions para Nano Server em 10 de abril de 2018.</p>

Versão	Alterações
2018.09.15	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 12 de setembro de 2018• AWS Tools for Windows PowerShell versão 3.3.343• EC2Launch versão 1.3.2000430• AWSDriver NVMe versão 1.3 0• Driver EC2 WinUtil versão 2.0.0 <p>Microsoft Windows Server 2016 Base Nano</p> <p>O acesso a todas as versões públicas de Windows_Server-2016-English-Nano-Base será removido em setembro de 2018. As informações adicionais sobre o ciclo de vida do Nano Server, incluindo detalhes sobre como executar o Nano Server como contêiner podem ser encontradas aqui: https://docs.microsoft.com/en-us/windows-server/get-started/nano-in-semi-annual-channel.</p>
2018.08.15	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 14 de agosto de 2018• AWS Tools for Windows PowerShell versão 3.3.335• As AMIs padrão agora usam o serviço NTP da Amazon no IP 169.254.169.123 para sincronização de horário. Para obter mais informações, consulte Configurações de NTP (Network Time Protocol) padrão para AMIs do Windows da Amazon (p. 603). <p>Microsoft Windows Server 2016 Base Nano</p> <p>O acesso a todas as versões públicas de Windows_Server-2016-English-Nano-Base será removido em setembro de 2018. As informações adicionais sobre o ciclo de vida do Nano Server, incluindo detalhes sobre como executar o Nano Server como contêiner podem ser encontradas aqui: https://docs.microsoft.com/en-us/windows-server/get-started/nano-in-semi-annual-channel.</p>
2018.07.11	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 10 de julho de 2018• EC2Config versão 4.9.2756• SSM Agent 2.2.800.0
22/06/2018	<p>Windows Server 2008 R2</p> <ul style="list-style-type: none">• Resolve um problema com as AMIs 2018.06.13 ao mudar uma instância de uma geração anterior para uma geração atual (por exemplo, M4 para M5).

Versão	Alterações
2018.06.13	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 12 de junho de 2018• EC2Config versão 4.9.2688• SSM Agent 2.2.619.0• AWS Tools for Windows PowerShell 3.3.283.0• AWSDriver do NVMe 1.2.0• AWS PV driver 8.2.3
09/05/2018	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 9 de maio de 2018• EC2Config versão 4.9.2644• SSM Agent 2.2.493.0• AWS Tools for Windows PowerShell 3.3.270.0 <p>Windows Server, versão 1709 e Windows Server, versão 1803</p> <ul style="list-style-type: none">• Agora, as AMIs estão disponíveis. Para obter mais informações, consulte AMIs do Windows Server versão 1709 e 1803 para Amazon EC2.
2018.04.11	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 10 de abril de 2018• EC2Config versão 4.9.2586• SSM Agent 2.2.392.0• AWS Tools for Windows PowerShell 3.3.256.0• AWS CloudFormationModelos 1.4.30• Configurações de Serial INF e Intel Chipset INF para suportar novos tipos de instância <p>SQL Server 2017</p> <ul style="list-style-type: none">• Atualização cumulativa 5 (CU5) <p>SQL Server 2016 SP1</p> <ul style="list-style-type: none">• Atualização cumulativa 8 (CU8)

Versão	Alterações
2018.03.24	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 13 de março de 2018 EC2Config versão 4.9.2565 SSM Agent 2.2.355.0 AWS Tools for Windows PowerShell 3.3.245.0 AWS PV driver 8.2 AWS ENA driver 1.2.3.0 Amazon EC2 Hibernate Agent 1.0 (reversão de 2.1.0 na versão 2018.03.16 da AMI) AWS EC2WinUtilDriver 1.0.1 (para a solução de problemas) <p>Windows Server 2016</p> <ul style="list-style-type: none"> EC2Launch 1.3.2000080
16/03/2018	A AWS removeu todas as AMIs do Windows com data de 16 de março de 2018 devido a um problema com um caminho sem aspas na configuração do Amazon EC2 Hibernate Agent. Para obter mais informações, consulte Problema com o Hibernate Agent (AMIs de 16 de março de 2018) (p. 38) .
2018.03.06	<p>Todas as AMIs</p> <ul style="list-style-type: none"> AWS PV driver 8.2.1
23/02/2018	<p>Todas as AMIs</p> <ul style="list-style-type: none"> AWS PV driver 7.4.6 (reversão de 8.2 na versão 2018.02.13 da AMI)
13/02/2018	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 13 de fevereiro de 2018 EC2Config versão 4.9.2400 SSM Agent 2.2.160.0 AWS Tools for Windows PowerShell 3.3.225.1 AWS PV driver 8.2 AWS ENA driver 1.2.3.0 AWSDriver do NVMe 1.0.0.146 Amazon EC2 HibernateAgent 1.0.0 <p>Windows Server 2016</p> <ul style="list-style-type: none"> EC2Launch 1.3.740
2018.01.12	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 9 de janeiro de 2018

Versão	Alterações
2018.01.05	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em janeiro de 2018• Configurações do registro para habilitar mitigações para as vulnerabilidades Spectre e Meltdown• AWS Tools for Windows PowerShell 3.3.215• EC2Config versão 4.9.2262

Atualizações mensais de AMI para 2017

Para obter mais informações sobre as atualizações da Microsoft, consulte [Descrição das alterações do conteúdo de serviços de atualização de software e do Windows Server para 2017](#).

Versão	Alterações
2017.12.13	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 12 de dezembro de 2017• EC2Config versão 4.9.2218• AWS CloudFormationModelos 1.4.27• AWSDriver do NVMe 1.02• SSM Agent 2.2.93.0• AWS Tools for Windows PowerShell 3.3.201
2017.11.29	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Componentes removidos para Volume Shadow Copy Service (VSS) incluído no 2017.11.18 e no 2017.11.19 devido a um problema de compatibilidade com o Backup do Windows.
19/11/2017	<p>Todas as AMIs</p> <ul style="list-style-type: none">• EC2 Hibernate Agent 1.0 (oferece suporte a hibernação em instâncias spot)
18/11/2017	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 14 de novembro de 2017• EC2Config versão 4.9.2218• SSM Agent 2.2.64.0• AWS Tools for Windows PowerShell 3.3.182• Driver Elastic Network Adapter (ENA) 1.08 (reversão de 1.2.2 na versão da AMI de 13/10/2017)• Consulta da AMI mais recente do Windows usando o Systems Manager Parameter Store <p>Windows Server 2016</p> <ul style="list-style-type: none">• EC2Launch 1.3.640

Versão	Alterações
13/10/2017	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 11 de outubro de 2017• EC2Config versão 4.9.2188• SSM Agent 2.2.30.0• AWS CloudFormationModelos 1.4.24• Driver Elastic Network Adapter (ENA) 1.2.2. (Windows Server 2008 R2 a Windows Server 2016)
04/10/2017	<p>Microsoft SQL Server</p> <p>Agora, as AMIs do Windows Server 2016 com Microsoft SQL Server 2017 permanecerão públicas em todas as regiões.</p> <ul style="list-style-type: none">• Windows_Server-2016-English-Full-SQL_2017_Enterprise-2017.10.04• Windows_Server-2016-English-Full-SQL_2017_Standard-2017.10.04• Windows_Server-2016-English-Full-SQL_2017_Web-2017.10.04• Windows_Server-2016-English-Full-SQL_2017_Express-2017.10.04 <p>O Microsoft SQL Server 2017 oferece suporte aos seguintes recursos:</p> <ul style="list-style-type: none">• Serviços de Machine Learning com suporte a Python (ML e AI) e idioma R• Ajuste automático de banco de dados• Grupos de disponibilidade sem clusters• Executados no Red Hat Enterprise Linux (RHEL), no SUSE Linux Enterprise Server (SLES) e no Ubuntu. Para obter mais informações, consulte o seguinte artigo da Microsoft: Diretrizes de instalação para SQL Server no Linux. Sem suporte no Amazon Linux.• Migrações entre sistemas operacionais Windows e Linux• Recompilação de índice online retomável• Processamento de consulta adaptável aprimorado• Suporte a dados de gráfico
13/09/2017	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 13 de setembro de 2017• EC2Config versão 4.9.2106• SSM Agent 2.0.952.0• AWS Tools for Windows PowerShell 3.3.143• AWS CloudFormationModelos 1.4.21

Versão	Alterações
09/08/2017	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 9 de agosto de 2017 EC2Config versão 4.9.2016 SSM Agent 2.0.879.0 <p>Windows Server 2012 R2</p> <ul style="list-style-type: none"> Devido a um erro interno, essas AMIs foram lançadas com uma versão mais antiga do AWS Tools for Windows PowerShell, 3.3.58.0.
2017.07.13	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 13 de julho de 2017 EC2Config versão 4.9.1981 SSM Agent 2.0.847.0 <p>Windows Server 2016</p> <ul style="list-style-type: none"> Driver SRIOV Intel 2.0.210.0
2017.06.14	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 14 de junho de 2017 Atualizações do .NET Framework 4.7 instaladas a partir do Windows Update As atualizações da Microsoft para corrigir o erro "privilegio não mantido" usando o cmdlet PowerShell Stop-Computer. Para obter mais informações, consulte Erro de privilégio não mantido no site da Microsoft. EC2Config versão 4.9.1900 SSM Agent 2.0.805.0 AWS Tools for Windows PowerShell 3.3.99.0 O Internet Explorer 11 para o desktop é o padrão, e não o Internet Explorer imersivo <p>Windows Server 2016</p> <ul style="list-style-type: none"> EC2Launch 1.3.610
30/05/2017	A AMI do Windows_Server-2008-SP2-English-32Bit-Base-2017.05.10 foi atualizada para a AMI do Windows_Server-2008-SP2-English-32Bit-Base-2017.05.30 para resolver um problema na geração de senhas.
22/05/2017	A AMI do Windows_Server-2016-English-Full-Base-2017.05.10 AMI foi atualizada para a AMI do Windows_Server-2016-English-Full-Base-2017.05.22 após alguma limpeza de log.

Versão	Alterações
2017.05.10	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 9 de maio de 2017• AWSDriver PV v7.4.6• AWS Tools for Windows PowerShell 3.3.83.0 <p>Windows Server 2016</p> <ul style="list-style-type: none">• SSM Agent 2.0.767
2017.04.12	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 11 de abril de 2017• AWS Tools for Windows PowerShell 3.3.71.0• AWS CloudFormationModelos 1.4.18 <p>Do Windows Server 2003 para Windows Server 2012</p> <ul style="list-style-type: none">• EC2Config versão 4.9.1775• SSM Agent 2.0.761.0 <p>Windows Server 2016</p> <ul style="list-style-type: none">• SSM Agent 2.0.730.0
2017.03.15	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 14 de março de 2017• atua AWS Tools for Windows PowerShell• Modelos AWS CloudFormation atuais <p>Do Windows Server 2003 para Windows Server 2012</p> <ul style="list-style-type: none">• EC2Config versão 4.7.1631• SSM Agent 2.0.682.0 <p>Windows Server 2016</p> <ul style="list-style-type: none">• SSM Agent 2.0.706.0• EC2Launch v1.3.540
21/02/2017	<p>A Microsoft anunciou recentemente que não lançará patches nem atualizações de segurança mensais em fevereiro. Todos os patches e atualizações de segurança de fevereiro serão incluídos na atualização de março.</p> <p>O Amazon Web Services não lançou AMIs atualizadas do Windows Server em fevereiro.</p>

Versão	Alterações
11/01/2017	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 10 de janeiro de 2017• atua AWS Tools for Windows PowerShell• Modelos AWS CloudFormation atuais <p>Do Windows Server 2003 para Windows Server 2012</p> <ul style="list-style-type: none">• EC2Config versão 4.2.1442• SSM Agent 2.0.599.0

Atualizações mensais de AMI para 2016

Para obter mais informações sobre as atualizações da Microsoft, consulte [Descrição das alterações do conteúdo de serviços de atualização de software e do Windows Server para 2016](#).

Versão	Alterações
2016.12.14	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em 13 de dezembro de 2016• atua AWS Tools for Windows PowerShell <p>Do Windows Server 2003 para Windows Server 2012</p> <ul style="list-style-type: none">• Lançado o EC2Config versão 4.1.1396• Driver do Elastic Network Adapter (ENA) 1.0.9.0 (somente para o Windows Server 2008 R2) <p>Windows Server 2016</p> <p>Novas AMIs disponíveis em todas as regiões:</p> <ul style="list-style-type: none">• Windows_Server-2016-English-Core-Base <p>Microsoft SQL Server</p> <p>Todas as AMIs do Microsoft SQL Server com o pacote de serviço mais recente agora são públicas em todas as regiões. Essas novas AMIs substituem as antigas AMIs de service pack do SQL</p> <ul style="list-style-type: none">• Windows_Server-2008-R2_SP1-English-64Bit-SQL_2012_SP3_edition-2016.12.14• Windows_Server-2012-RTM-English-64Bit-SQL_2012_SP3_edition-2016.12.14• Windows_Server-2012-R2_RTM-English-64Bit-SQL_2014_SP2_edition-2016.12.14• Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP2_edition-2016.12.14

Versão	Alterações
	<ul style="list-style-type: none"> Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_SP1_<i>edition</i>-2016.12.14 Windows_Server-2016-English-Full-SQL_2016_SP1_<i>edition</i>-2016.12.14 <p>O SQL Server 2016 SP1 é uma versão principal. Os seguintes recursos, que estavam disponíveis anteriormente somente na edição Enterprise agora estão habilitados nas edições Standard, Web e Express com o SQL Server 2016 SP1:</p> <ul style="list-style-type: none"> Segurança no nível da linha Mascaramento dinâmico de dados Captura de dados de alteração Snapshot do banco de dados Armazenamento personalizado Particionamento Compactação Em Memory OLTP Sempre criptografado
23/11/2016	<p>Do Windows Server 2003 para Windows Server 2012</p> <ul style="list-style-type: none"> Lançado o EC2Config versão 4.1.1378 As AMIs lançadas neste mês em diante usam o serviço EC2Config para processar configurações na hora da inicialização e o SSM Agent para processar solicitações Config e do Run Command do AWS Systems Manager. O EC2Config não processa mais solicitações para o State Manager e o Run Command do Systems Manager. O instalador mais recente do EC2Config instala o SSM Agent lado a lado com o serviço EC2Config. Para obter mais informações, consulte Configurar uma instância do Windows usando o serviço EC2Config (p. 530).
2016.11.09	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 8 de novembro de 2016 Lançado o driver AWS PV, versão 7.4.3.0 para Windows 2008 R2 e posterior atua AWS Tools for Windows PowerShell
18/10/2016	<p>Todas as AMIs</p> <ul style="list-style-type: none"> Atualizações de segurança da Microsoft vigentes em 12 de outubro de 2016 atua AWS Tools for Windows PowerShell <p>Windows Server 2016</p> <ul style="list-style-type: none"> Lançadas AMIs para Windows Server 2016. Essas AMIs incluem alterações significativas. Por exemplo, elas não incluem o serviço EC2Config. Para obter mais informações, consulte Alterações nas AMIs do Windows Server 2016 e posterior (p. 37).

Versão	Alterações
14/09/2016	Todas as AMIs <ul style="list-style-type: none"> • Atualizações de segurança da Microsoft vigentes em 13 de setembro de 2016 • atua AWS Tools for Windows PowerShell • A AMI do Windows_Server-2012-RTM-Japanese-64Bit-SQL_2008_R3_SP2_Standard foi renomeada para Windows_Server-2012-RTM-Japanese-64Bit-SQL_2008_R2_SP3_Standard
26/08/2016	Todas as AMIs do Windows Server 2008 R2 datadas de 2016.08.11 foram atualizadas para corrigir um problema conhecido. As novas AMIs são datadas de 2016.08.25.
11/08/2016	Todas as AMIs <ul style="list-style-type: none"> • Ec2Config v3.19.1153 • Atualizações de segurança da Microsoft vigentes em 10 de agosto de 2016 • Habilitada o recurso de fortalecimento do handler de exceção User32 da chave de Registro no Internet Explorer para MS15-124 <p>Windows Server 2008 R2, Windows Server 2012 RTM e Windows Server 2012 R2</p> <ul style="list-style-type: none"> • Driver do Elastic Network Adapter (ENA) 1.0.8.0 • Propriedade de ENA AMI definida como habilitada • AWSO driver PV para Windows Server 2008 R2 foi relançado neste mês devido a um problema conhecido. As AMIs do Windows Server 2008 R2 foram removidas em julho devido a esse problema.
02/08/2016	Todas as AMIs do Windows Server 2008 R2 para julho foram removidas e distribuídas nas AMIs datadas de 2016.06.15, devido a um problema descoberto no driver AWS PV. O problema no driver AWS PV foi corrigido. O lançamento de AMIs de agosto incluirá AMIs do Windows Server 2008 R2 com o driver AWS PV corrigido e as atualizações de julho/agosto do Windows.
26/07/2016	Todas as AMIs <ul style="list-style-type: none"> • Ec2Config v3.18.1118 • As AMIs de 2016.07.13 não estavam presentes nos patches de segurança. Foi reaplicado o patch às AMIs. Processos adicionais foram implementados para verificar instalações bem-sucedidas de patches daqui em diante.
13/07/2016	Todas as AMIs <ul style="list-style-type: none"> • Atualizações de segurança da Microsoft vigentes em julho de 2016 • atua AWS Tools for Windows PowerShell • Driver AWS PV 7.4.2.0 atualizado • AWSDriver PV para Windows Server 2008 R2

Versão	Alterações
16/06/2016	<p>Todas as AMIs</p> <ul style="list-style-type: none"> • Atualizações de segurança da Microsoft vigentes em junho de 2016 • atua AWS Tools for Windows PowerShell • Serviço EC2Config versão 3.17.1032 <p>Microsoft SQL Server</p> <ul style="list-style-type: none"> • Lançadas 10 AMIs que incluem versões de 64 bits do Microsoft SQL Server 2016. Se estiver usando o console do Amazon EC2, vá até Images (Imagens), AMIs, Public Images (Imagens públicas) e digite Windows_Server-2012-R2_RTM-English-64Bit-SQL_2016_Standard na barra de pesquisa. Para obter mais informações, consulte Novidades no SQL Server 2016 no MSDN.
11/05/2016	<p>Todas as AMIs</p> <ul style="list-style-type: none"> • Atualizações de segurança da Microsoft vigentes em maio de 2016 • atua AWS Tools for Windows PowerShell • Serviço EC2Config versão 3.16.930 • Patch do MS15-011 Active Directory instalado <p>Windows Server 2012 R2</p> <ul style="list-style-type: none"> • Driver SRIOV Intel 1.0.16.1
13/04/2016	<p>Todas as AMIs</p> <ul style="list-style-type: none"> • Atualizações de segurança da Microsoft vigentes em abril de 2016 • atua AWS Tools for Windows PowerShell • Serviço EC2Config versão 3.15.880
09/03/2016	<p>Todas as AMIs</p> <ul style="list-style-type: none"> • Atualizações de segurança da Microsoft vigentes em março de 2016 • atua AWS Tools for Windows PowerShell • Serviço EC2Config versão 3.14.786
10/02/2016	<p>Todas as AMIs</p> <ul style="list-style-type: none"> • Atualizações de segurança da Microsoft vigentes em fevereiro de 2016 • atua AWS Tools for Windows PowerShell • Serviço EC2Config versão 3.13.727
25/01/2016	<p>Todas as AMIs</p> <ul style="list-style-type: none"> • Atualizações de segurança da Microsoft vigentes em janeiro de 2016 • atua AWS Tools for Windows PowerShell • Serviço EC2Config versão 3.12.649
05/01/2016	<p>Todas as AMIs</p> <ul style="list-style-type: none"> • atua AWS Tools for Windows PowerShell

Atualizações mensais de AMI para 2015

Para obter mais informações sobre as atualizações da Microsoft, consulte [Descrição das alterações do conteúdo de serviços de atualização de software e do Windows Server para 2015](#).

Versão	Alterações
15/12/2015	Todas as AMIs <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em dezembro de 2015• atua AWS Tools for Windows PowerShell
11/11/2015	Todas as AMIs <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em novembro de 2015• atua AWS Tools for Windows PowerShell• Serviço EC2Config versão 3.11.521• CFN Agent atualizado para a versão mais recente
26/10/2015	Corrigidos os tamanhos do volume de inicialização de AMIs básicas para 30 GB em vez de 35 GB
14/10/2015	Todas as AMIs <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em outubro de 2015• Serviço EC2Config versão 3.10.442• atua AWS Tools for Windows PowerShell• Atualizados os Service Packs do SQL para as versões mais recentes de todas as variantes do SQL• Removidas as entradas antigas de logs no evento• Os nomes das AMIs foram alterados para refletir o service pack mais recente. Por exemplo, a AMI mais recente com o Server 2012 e o SQL 2014 Standard é chamada de "Windows_Server-2012-RTM-English-64Bit-SQL_2014_SP1_Standard-2015.10.26", não "Windows_Server-2012-RTM-English-64Bit-SQL_2014_RTM_Standard-2015.10.26".
09/09/2015	Todas as AMIs <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em setembro de 2015• Serviço EC2Config versão 3.9.359• atua AWS Tools for Windows PowerShell• Scripts auxiliares AWS CloudFormation atuais
18/08/2015	Todas as AMIs <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em agosto de 2015• Serviço EC2Config versão 3.8.294• atua AWS Tools for Windows PowerShell <p>Somente AMIs com o Windows Server 2012 e o Windows Server 2012 R2</p> <ul style="list-style-type: none">• AWSDriver PV 7.3.2

Versão	Alterações
21/07/2015	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em julho de 2015• Serviço EC2Config versão 3.7.308• atua AWS Tools for Windows PowerShell• Modificadas as descrições de AMIs de imagens SQL para fins de consistência
10/06/2015	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em junho de 2015• Serviço EC2Config versão 3.6.269• atua AWS Tools for Windows PowerShell• Scripts auxiliares AWS CloudFormation atuais <p>Somente AMIs com o Windows Server 2012 R2</p> <ul style="list-style-type: none">• AWSDriver PV 7.3.1
13/05/2015	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em maio de 2015• Serviço EC2Config versão 3.5.228• atua AWS Tools for Windows PowerShell
15/04/2015	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em abril de 2015• Serviço EC2Config versão 3.3.174• atua AWS Tools for Windows PowerShell
11/03/2015	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em março de 2015• Serviço EC2Config versão 3.2.97• atua AWS Tools for Windows PowerShell <p>Somente AMIs com o Windows Server 2012 R2</p> <ul style="list-style-type: none">• AWSDriver PV 7.3.0
11/02/2015	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em fevereiro de 2015• Serviço EC2Config versão 3.0.54• atua AWS Tools for Windows PowerShell• Scripts auxiliares AWS CloudFormation atuais

Versão	Alterações
14/01/2015	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em janeiro de 2015• Serviço EC2Config versão 2.3.313• atua AWS Tools for Windows PowerShell• Scripts auxiliares AWS CloudFormation atuais

Atualizações mensais de AMI para 2014

Para obter mais informações sobre as atualizações da Microsoft, consulte [Descrição das alterações do conteúdo de serviços de atualização de software e do Windows Server para 2014](#).

Versão	Alterações
10/12/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em dezembro de 2014• Serviço EC2Config versão 2.2.12• atua AWS Tools for Windows PowerShell
19/11/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em novembro de 2014• Serviço EC2Config versão 2.2.11• atua AWS Tools for Windows PowerShell
15/10/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em outubro de 2014• Serviço EC2Config versão 2.2.10• atua AWS Tools for Windows PowerShell <p>Somente AMIs com o Windows Server 2012 R2</p> <ul style="list-style-type: none">• AWSDriver PV 7.2.4.1 (resolve os problemas com a Limpeza de Plug and Play, que agora é habilitada por padrão)
10/09/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em setembro de 2014• Serviço EC2Config versão 2.2.8• atua AWS Tools for Windows PowerShell <p>Somente AMIs com o Windows Server 2012 R2</p> <ul style="list-style-type: none">• Desabilitada a limpeza de Plug and Play (consulte Informações importantes)• AWSO Driver PV 7.2.2.1 (resolve problemas com o desinstalador)

Versão	Alterações
13/08/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em agosto de 2014• Serviço EC2Config versão 2.2.7• atua AWS Tools for Windows PowerShell <p>Somente AMIs com o Windows Server 2012 R2</p> <ul style="list-style-type: none">• AWSO Driver PV 7.2.2.1 (melhora a performance do disco, resolve problemas na reconexão de várias interfaces de rede e configurações perdidas de rede)
10/07/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em julho de 2014• Serviço EC2Config versão 2.2.5• atua AWS Tools for Windows PowerShell
12/06/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em junho de 2014• Serviço EC2Config versão 2.2.4• Removidos os drivers NVIDIA (exceto AMIs do Windows Server 2012 R2)• atua AWS Tools for Windows PowerShell
14/05/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em maio de 2014• Serviço EC2Config versão 2.2.2• atua AWS Tools for Windows PowerShell• AWS CloudFormationScripts auxiliares versão 1.4.0
09/04/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em abril de 2014• atua AWS Tools for Windows PowerShell• Scripts auxiliares AWS CloudFormation atuais
12/03/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em março de 2014

Versão	Alterações
12/02/2014	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em fevereiro de 2014• Serviço EC2Config versão 2.2.1• atua AWS Tools for Windows PowerShell• KB2634328• Removido o valor BCDEdit useplatformclock <p>Somente AMIs com o Microsoft SQL Server</p> <ul style="list-style-type: none">• Pacote de atualizações cumulativas 8 do Microsoft SQL Server 2012 SP1• Pacote de atualizações cumulativas 10 do Microsoft SQL Server 2008 R2

Atualizações mensais de AMI para 2013

Versão	Alterações
13/11/2013	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em novembro de 2013• Serviço EC2Config versão 2.1.19• atua AWS Tools for Windows PowerShell• Configurado o NTP para sincronizar a hora uma vez por dia (o padrão é a cada sete dias) <p>Somente AMIs com o Windows Server 2012</p> <ul style="list-style-type: none">• Limpa a pasta WinSXS usando o seguinte comando: <code>dism /online / cleanup-image /StartComponentCleanup</code>
11/09/2013	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em setembro de 2013• Serviço EC2Config versão 2.1.18• atua AWS Tools for Windows PowerShell• AWS CloudFormationScripts auxiliares versão 1.3.15
10/07/2013	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em julho de 2013• Serviço EC2Config versão 2.1.16• Expandido o volume raiz para 50 GB• Definido o arquivo de página como 512 MB, expandindo para 8 GB, conforme necessário• atua AWS Tools for Windows PowerShell
12/06/2013	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em junho de 2013

Versão	Alterações
	<ul style="list-style-type: none">• atua AWS Tools for Windows PowerShell <p>Somente AMIs com o Microsoft SQL Server</p> <ul style="list-style-type: none">• Microsoft SQL Server 2012 SP1 com pacote de atualizações cumulativas 4
15/05/2013	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em maio de 2013• Serviço EC2Config versão 2.1.15• Todos os volumes de armazenamento de instâncias anexados por padrão• PowerShell remoto habilitado por padrão• atua AWS Tools for Windows PowerShell
14/04/2013	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em abril de 2013• atua AWS Tools for Windows PowerShell• AWS CloudFormationScripts auxiliares versão 1.3.14
14/03/2013	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em março de 2013• Serviço EC2Config versão 2.1.14• Citrix Agent com correção de pulsação de CPU• atua AWS Tools for Windows PowerShell• AWS CloudFormationScripts auxiliares versão 1.3.11
22/02/2013	<p>Todas as AMIs</p> <ul style="list-style-type: none">• Atualizações de segurança da Microsoft vigentes em fevereiro de 2013• KB2800213• Atualização do Windows PowerShell 3.0• Serviço EC2Config versão 2.1.13• Citrix Agent com correção do tempo• Drivers do Citrix PV datado de 2011.07.19• atua AWS Tools for Windows PowerShell• AWS CloudFormationScripts auxiliares versão 1.3.8 <p>Somente AMIs com o Microsoft SQL Server</p> <ul style="list-style-type: none">• Pacote de atualizações cumulativas 5 do Microsoft SQL Server 2012

Atualizações mensais de AMI para 2012

Versão	Alterações
12/12/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em dezembro de 2012Definido o valor de Registro ActiveTimeBias como 0Desabilitado o IPv6 para o adaptador de redeServiço EC2Config versão 2.1.9Adicionado o AWS Tools for Windows PowerShell e definida a política para permitir a importação de módulo
15/11/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em novembro de 2012Serviço EC2Config versão 2.1.7
10/10/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em outubro de 2012
15/08/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em agosto de 2012Serviço EC2Config versão 2.1.2KB2545227
11/07/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em julho de 2012
12/06/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em junho de 2012Definido o arquivo de página como 4 GBRemovidos os pacotes de idioma instaladosDefinida a opção de performance como "Ajustar para melhor performance"Definido o protetor de tela para não exibir mais a tela de logon ao retomarRemovidas as versões anteriores do driver do RedHat usando pnputilRemovidos os bootloaders duplicados e definida a bootstatuspolicy como ignoreallfailures usando bcdedit
10/05/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em maio de 2012Serviço EC2Config versão 2.1.0
11/04/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em abril de 2012KB2582281Versão atual do EC2ConfigHora do sistema em UTC em vez de GMT

Versão	Alterações
13/03/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em março de 2012
24/02/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em fevereiro de 2012Padronizados os nomes e as descrições das AMIs
12/01/2012	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em janeiro de 2012Driver do RedHat PV versão 1.3.10

Atualizações mensais de AMI para 2011 e anos anteriores

Versão	Alterações
11/09/2011	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança da Microsoft vigentes em setembro de 2011
1.04	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança vigentes da MicrosoftAtualizado o driver de redeCorrigido o problema em instâncias em uma VPC que perdiam a conectividade quando o fuso horário da instância era alterado
1.02	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança vigentes da MicrosoftAtualizado o driver de redeAdicionado suporte para a ativação de licenciamento para instâncias em uma VPC
1.01	Todas as AMIs <ul style="list-style-type: none">Atualizações de segurança vigentes da MicrosoftCorrigido o problema senhas geradas incorretamente ao aguardar pela disponibilidade de rede
1,0	Todas as AMIs <ul style="list-style-type: none">Versão inicial

Localizar uma AMI do Windows

Antes de executar uma instância, você deve selecionar AMIs para usar. Ao selecionar a AMI, considere os seguintes requisitos que podem existir para as instâncias que você executará:

- A região
- O sistema operacional
- A arquitetura 32 bits (`i386`) ou 64 bits (`x86_64`)
- O provedor (por exemplo, Amazon Web Services)
- Software adicional (por exemplo, SQL Server)

Se você precisar localizar uma AMI do Linux, consulte [Find a Linux AMI](#) (Localizar AMI do Linux) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

- [Localizar uma AMI do Windows usando o console do Amazon EC2 \(p. 103\)](#)
- [Localizar uma AMI usando o AWS Tools for Windows PowerShell \(p. 104\)](#)
- [Localizar uma AMI usando o AWS CLI \(p. 104\)](#)
- [Localizar a AMI do Windows mais recente usando o Systems Manager \(p. 105\)](#)
- [Use um parâmetro de Systems Manager para localizar uma AMI \(p. 105\)](#)

Localizar uma AMI do Windows usando o console do Amazon EC2

Você pode encontrar AMIs do Windows usando o console do Amazon EC2. Você pode selecionar na lista de AMIs ao usar o assistente de execução para executar uma instância ou pesquisar todas as AMIs disponíveis usando a página [Images](#) (Imagens). Os IDs da AMI são exclusivos de cada região da AWS.

Como localizar uma AMI do Windows usando o Launch Wizard

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel do console, selecione Launch instance (Executar instância).
4. Na guia Quick Start (Início rápido), selecione uma das AMIs mais usadas na lista. Se você não encontrar a AMI necessária, selecione a guia My AMIs (Minhas AMIs), AWS Marketplace ou Community AMIs (AMIs da comunidade) para localizar AMIs adicionais. Para obter mais informações, consulte [Etapa 1: Escolher uma imagem de máquina da Amazon \(AMI\) \(p. 419\)](#).

Para localizar uma AMI do Windows usando a página [Images](#)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel de navegação, selecione AMIs.
4. (Opcional) Use as opções de Filter para restringir o escopo da lista de AMIs exibidas e ver somente as AMIs que lhe interessam. Por exemplo, para listar todas as AMIs do Windows fornecidas pela AWS, selecione Public images (Imagens públicas). Escolha a barra de pesquisa e selecione Owner no menu, depois selecione Amazon images. Escolha a barra de pesquisa novamente para selecionar Platform e, depois, o sistema operacional na lista fornecida.
5. (Opcional) Escolha o ícone Show/Hide Columns para selecionar quais atributos de imagens serão exibidos, como o tipo de dispositivo raiz. Como alternativa, você pode selecionar uma AMI na lista e visualizar suas propriedades na guia Details.

-
6. Para executar uma instância dessa AMI, selecione-a e escolha Launch. Para obter mais informações sobre como executar uma instância usando o console, consulte [Execução da instância de uma AMI \(p. 420\)](#). Se você não estiver pronto para executar a instância agora, anote o ID da AMI para consultar depois.

Localizar uma AMI usando o AWS Tools for Windows PowerShell

Você pode usar cmdlets no Amazon EC2 ou no AWS Systems Manager para listar somente as AMIs do Windows que atendam às necessidades. Depois de localizar uma AMI que atenda às necessidades, anote o ID de maneira que você possa usá-la para executar instâncias. Para obter mais informações, consulte [Launch an Instance Using Windows PowerShell](#) (Executar uma instância usando o Windows PowerShell) no AWS Tools for Windows PowerShell User Guide (Manual do usuário do AWS Tools for Windows PowerShell).

Amazon EC2

Para obter informações e exemplos, consulte [Find an AMI Using Windows PowerShell](#) (Encontrar uma AMI usando o Windows PowerShell) no AWS Tools for Windows PowerShell User Guide (Manual do usuário do AWS Tools for Windows PowerShell).

Systems Manager Parameter Store

Para obter informações e exemplos, consulte [Consultar a AMI do Windows mais recente usando a Systems Manager Parameter Store](#).

Localizar uma AMI usando o AWS CLI

Você pode usar comandos da AWS CLI do Amazon EC2 ou AWS Systems Manager para listar somente as AMIs do Windows que atendam às necessidades. Depois de localizar uma AMI que atenda às necessidades, anote o ID de maneira que você possa usá-la para executar instâncias. Para obter mais informações, consulte [Launching an Instance Using the AWS CLI](#) (Executar uma instância usando a AWS CLI) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).

Amazon EC2

O comando `describe-images` oferece suporte à filtragem de parâmetros. Por exemplo, use o parâmetro `--owners` para exibir AMIs públicas de propriedade da Amazon.

```
aws ec2 describe-images --owners self amazon
```

Você pode adicionar o seguinte filtro ao comando anterior para exibir somente AMIs do Windows:

```
--filters "Name=platform,Values=windows"
```

Important

Omitir o sinalizador `--owners` no comando `describe-images` retornará todas as imagens para as quais você tem permissões de execução, independentemente da propriedade.

Systems Manager Parameter Store

Para obter informações e exemplos, consulte [Consultar a AMI do Windows mais recente usando a Systems Manager Parameter Store](#).

Localizar a AMI do Windows mais recente usando o Systems Manager

O Amazon EC2 fornece parâmetros públicos do AWS Systems Manager para AMIs públicas mantidas pela AWS que podem ser usados ao executar instâncias.

Os parâmetros públicos de AMI do Amazon EC2 estão disponíveis nos seguintes caminhos:

/aws/service/ami-windows-latest

Você pode visualizar uma lista de todas as AMIs do Windows na região da AWS atual usando o seguinte comando na CLI da AWS.

```
aws ssm get-parameters-by-path --path /aws/service/ami-windows-latest --query "Parameters[ ].Name"
```

Para obter mais informações, consulte [Using public parameters](#) (Usar parâmetros públicos) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager) e [Query for the Latest Windows AMI Using AWS Systems Manager Parameter Store](#) (Consultar a AMI do Windows mais recente usando o repositório de parâmetros do AWS Systems Manager).

Use um parâmetro de Systems Manager para localizar uma AMI

Ao executar uma instância usando o assistente de execução do EC2 no console, você pode selecionar uma AMI na lista ou selecionar um parâmetro do AWS Systems Manager que aponte para um ID de AMI. Se usar o código de automação para executar as instâncias, você poderá especificar o parâmetro do Systems Manager em vez do ID de AMI.

Um parâmetro do Systems Manager é um par de chave-valor definido pelo cliente que pode ser criado no repositório de parâmetros do Systems Manager. O repositório de parâmetros fornece um armazenamento central para externalizar os valores de configuração da aplicação. Para obter mais informações, consulte [AWS Systems Manager Parameter Store](#) (Repositório de parâmetros do AWS Systems Manager), no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

Ao criar um parâmetro que aponte para um ID de AMI, especifique o tipo de dado como `aws:ec2:image`. Esse tipo de dado garante que o valor do parâmetro seja validado como ID da AMI ao ser criado ou modificado. Para obter mais informações, consulte [Suporte a parâmetro nativo para IDs de imagem de máquina da Amazon](#) no Guia do usuário do AWS Systems Manager.

Tópicos

- [Casos de uso \(p. 105\)](#)
- [Executar uma instância usando um parâmetro de Systems Manager \(p. 106\)](#)
- [Permissions \(p. 107\)](#)
- [Limitations \(p. 107\)](#)

Casos de uso

Ao usar os parâmetros do Systems Manager de modo a apontar para IDs de AMI, é possível facilitar, para os usuários, a seleção da AMI correta ao executar instâncias, e simplificar a manutenção do código de automação.

Mais fácil para os usuários

Se você precisar que as instâncias sejam executadas usando uma AMI específica, e se essa AMI for atualizada regularmente, recomendamos que você exija que os usuários selezionem um parâmetro do Systems Manager para localizar a AMI. Ao exigir que os usuários selezionem um parâmetro do Systems Manager, é possível garantir que a AMI mais recente seja usada para executar instâncias.

Por exemplo, todo mês você pode criar em sua organização uma versão da AMI que tenha os patches mais recentes do sistema operacional e da aplicação. Além disso, exija que os usuários executem instâncias usando a versão mais recente da AMI. Para garantir que os usuários usem a versão mais recente, você pode criar um parâmetro do Systems Manager (por exemplo, `golden-ami`) que aponte para o ID da AMI correta. Toda vez que uma versão da AMI é criada, você atualiza o valor do ID de AMI no parâmetro para que ele sempre aponte para a AMI mais recente. Os usuários não precisam saber sobre as atualizações periódicas da AMI, porque eles continuarão selecionando sempre o mesmo parâmetro do Systems Manager. Ao fazer com que os usuários selezionem um parâmetro do Systems Manager, você facilita a seleção da AMI correta para uma execução da instância.

Simplificar a manutenção do código de automação

Se usar o código de automação para executar as instâncias, você poderá especificar o parâmetro do Systems Manager em vez do ID de AMI. Se uma versão da AMI for criada, altere o valor do ID de AMI no parâmetro para que ele aponte para a AMI mais recente. O código de automação que faz referência ao parâmetro não precisa ser modificado toda vez que uma versão da AMI é criada. Isso simplifica muito a manutenção da automação e ajuda a reduzir os custos de implantação.

Note

As instâncias em execução não são afetadas quando você altera o ID da AMI para o qual o parâmetro do Systems Manager aponta.

Executar uma instância usando um parâmetro de Systems Manager

Você pode executar uma instância usando o console ou a AWS CLI. Em vez de especificar um ID de AMI, você pode especificar um parâmetro do AWS Systems Manager que aponte para um ID de AMI.

Como localizar uma AMI do Windows usando um parâmetro do Systems Manager (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel do console, selecione Launch instance (Executar instância).
4. Escolha Search by Systems Manager parameter (Pesquisar por parâmetro do Systems Manager) (no canto superior direito).
5. Em Systems Manager parameter (Parâmetro do Systems Manager), selecione um parâmetro. O ID da AMI correspondente é exibido ao lado de Currently resolves to (Resolve atualmente para).
6. Escolha Pesquisar. As AMIs correspondentes ao ID da AMI são exibidas na lista.
7. Selecione a AMI na lista e escolha Select (Selecionar).

Para obter mais informações sobre como executar uma instância a partir de uma AMI usando o assistente de execução, consulte [Etapa 1: Escolher uma imagem de máquina da Amazon \(AMI\) \(p. 419\)](#).

Como executar uma instância usando um parâmetro do AWS Systems Manager em vez de um ID da AMI (AWS CLI)

O exemplo a seguir usa o parâmetro do Systems Manager `golden-ami` para executar uma instância `m5.xlarge`. O parâmetro aponta para um ID de AMI.

Para especificar o parâmetro no comando, use a seguinte sintaxe: `resolve:ssm:/parameter-name`, onde `resolve:ssm` é o prefixo padrão e `parameter-name` é o nome do parâmetro exclusivo. Observe que o nome do parâmetro faz distinção entre maiúsculas e minúsculas. As barras invertidas para o nome do parâmetro só são necessárias quando o parâmetro faz parte de uma hierarquia, por exemplo, `/amis/production/golden-ami`. Será possível omitir a barra invertida se o parâmetro não fizer parte de uma hierarquia.

No exemplo, os parâmetros `--count` e `--security-group` não são incluídos. Para `--count`, o padrão é 1. Se você tiver uma VPC e um grupo de segurança padrão, eles serão usados.

```
aws ec2 run-instances
  --image-id resolve:ssm:/golden-ami
  --instance-type m5.xlarge
  ...
```

Como executar uma instância usando uma versão específica de um parâmetro do AWS Systems Manager (AWS CLI)

Os parâmetros do Systems Manager são compatíveis com versão. Cada iteração de um parâmetro recebe um número de versão exclusivo. Você pode referenciar a versão do parâmetro da seguinte forma `resolve:ssm:parameter-name:version`, onde `version` é o número de versão exclusivo. Por padrão, a versão mais recente do parâmetro é usada quando nenhuma versão é especificada.

O exemplo a seguir usa a versão 2 do parâmetro.

No exemplo, os parâmetros `--count` e `--security-group` não são incluídos. Para `--count`, o padrão é 1. Se você tiver uma VPC e um grupo de segurança padrão, eles serão usados.

```
aws ec2 run-instances
  --image-id resolve:ssm:/golden-ami:2
  --instance-type m5.xlarge
  ...
```

Como executar uma instância usando um parâmetro público fornecido pela AWS

O Amazon EC2 fornece parâmetros públicos do Systems Manager para AMIs públicas fornecidas pela AWS. Por exemplo, o parâmetro público `/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2` está disponível em todas as regiões e sempre aponta para a versão mais recente da AMI do Amazon Linux 2 na região.

```
aws ec2 run-instances
  --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2
  --instance-type m5.xlarge
  ...
```

Permissions

Se usar parâmetros do Systems Manager que apontem para IDs de AMI no assistente de execução de instância, você deve adicionar `ssm:DescribeParameters` e `ssm:GetParameters` à política do IAM. `ssm:DescribeParameters` concede aos usuários do IAM permissão para visualizar e selecionar parâmetros do Systems Manager. `ssm:GetParameters` concede aos usuários do IAM a permissão para obter os valores dos parâmetros do Systems Manager. Também é possível restringir o acesso a parâmetros específicos do Systems Manager. Para obter mais informações, consulte [Usar o assistente de execução do EC2 \(p. 1187\)](#).

Limitations

As AMIs e os parâmetros do Systems Manager são específicos da região. Para usar o mesmo nome de parâmetro do Systems Manager entre regiões, crie um parâmetro do Systems Manager em cada região

com o mesmo nome (por exemplo, `golden-ami`). Em cada região, aponte o parâmetro do Systems Manager para uma AMI nessa região.

AMIs compartilhadas

Uma AMI compartilhada é uma AMI que um desenvolvedor criou e disponibilizou para que outros desenvolvedores usem. Uma das maneiras mais fáceis de começar a usar o Amazon EC2 é usar AMIs compartilhadas com os componentes necessários e adicionar o conteúdo personalizado. Você também pode criar suas próprias AMIs e compartilhá-las com outros.

Use a AMI compartilhada sob seu próprio risco. A Amazon não pode responsabilizar-se pela integridade ou segurança das AMIs compartilhadas por outros usuários do Amazon EC2. Portanto, trate as AMIs compartilhadas como você faria com qualquer código estranho que considere implantar no seu próprio datacenter e execute a investigação aplicável. Recomendamos que você obtenha AMIs de origens confiáveis.

As imagens públicas da Amazon têm um proprietário com alias, que aparece como `amazon` no campo da conta. Isso permite que você encontre AMIs da Amazon facilmente. Outros usuários não podem dar um alias às AMIs deles.

Para obter informações sobre como criar uma AMI, consulte [Criação de uma AMI personalizada do Windows](#). Para obter informações sobre como criar, fornecer e manter suas aplicações no AWS Marketplace , consulte a [Documentação do AWS Marketplace](#) .

Tópicos

- [Encontrar AMIs compartilhadas \(p. 108\)](#)
- [Tornar um AMI pública \(p. 110\)](#)
- [Compartilhar uma AMI com contas específicas da AWS \(p. 112\)](#)
- [Usar marcadores \(p. 114\)](#)
- [Melhores práticas para AMIs compartilhadas do Windows \(p. 115\)](#)

Encontrar AMIs compartilhadas

Você pode usar o console do Amazon EC2 ou a linha de comando para encontrar AMIs compartilhadas.

As AMIs são um recurso regional. Portanto, ao pesquisar uma AMI compartilhada (pública ou privada), é necessário procurá-la dentro da região onde ela está sendo compartilhada. Para disponibilizar uma AMI em uma região diferente, copie a AMI para a região e compartilhe-a. Para obter mais informações, consulte [Copiar um AMI \(p. 120\)](#).

Tópicos

- [Encontrar uma AMI compartilhada \(console\) \(p. 108\)](#)
- [Localizar uma AMI compartilhada \(Tools for Windows PowerShell\) \(p. 109\)](#)
- [Localizar uma AMI compartilhada \(AWS CLI\) \(p. 110\)](#)

Encontrar uma AMI compartilhada (console)

Para encontrar uma AMI privada usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione AMIs.

3. No primeiro filtro, escolha Imagens privadas. Estarão na lista todas as AMIs compartilhadas com você. Para granular sua pesquisa, selecione a barra de pesquisa e use as opções de filtro fornecidas no menu.

Para encontrar uma AMI pública usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione AMIs.
3. No primeiro filtro, escolha Imagens públicas. Para granular sua pesquisa, selecione a barra de pesquisa e use as opções de filtro fornecidas no menu.
4. Use filtros para listar somente os tipos de AMIs que lhe interessarem. Por exemplo, escolha Proprietário: e, então, Imagens da Amazon para exibir somente as imagens públicas da Amazon.

Localizar uma AMI compartilhada (Tools for Windows PowerShell)

Use o comando `Get-EC2Image` (Tools for Windows PowerShell) para listar as AMIs. Você pode direcionar o escopo da lista para os tipos de AMI que lhe interessam, conforme exibido nos exemplos a seguir.

Exemplo: Listar todas as AMIs públicas

O comando a seguir lista todas as AMIs públicas, inclusive todas as AMIs públicas de sua propriedade.

```
PS C:\> Get-EC2Image -ExecutableUser all
```

Exemplo: Listar AMIs permissões de execução explícita

O comando a seguir lista as AMIs para as quais você tenha permissões de execução explícita. Essa lista não inclui nenhuma AMI de sua propriedade.

```
PS C:\> Get-EC2Image -ExecutableUser self
```

Exemplo: Listar AMIs de propriedade da Amazon

O comando a seguir lista as AMIs de propriedade da Amazon. As AMIs públicas da Amazon têm um proprietário com alias, que aparece como `amazon` no campo da conta. Isso permite que você encontre AMIs da Amazon facilmente. Outros usuários não podem dar um alias às AMIs deles.

```
PS C:\> Get-EC2Image -Owner amazon
```

Exemplo: Listar AMIs de propriedade de uma conta

O comando a seguir lista as AMIs de propriedade da conta AWS específica.

```
PS C:\> Get-EC2Image -Owner 123456789012
```

Exemplo: Definir escopo das AMIs usando um filtro

Para reduzir o número de AMIs exibidas, use um filtro para listar somente os tipos de AMI que lhe interessam. Por exemplo, use o filtro a seguir para exibir somente AMIs com EBS.

```
-Filter @{ Name="root-device-type"; Values="ebs" }
```

Localizar uma AMI compartilhada (AWS CLI)

Use o comando `describe-images` (AWS CLI) para listar as AMIs. Você pode direcionar o escopo da lista para os tipos de AMI que lhe interessam, conforme exibido nos exemplos a seguir.

Exemplo: Listar todas as AMIs públicas

O comando a seguir lista todas as AMIs públicas, inclusive todas as AMIs públicas de sua propriedade.

```
aws ec2 describe-images --executable-users all
```

Exemplo: Listar AMIs permissões de execução explícita

O comando a seguir lista as AMIs para as quais você tenha permissões de execução explícita. Essa lista não inclui nenhuma AMI de sua propriedade.

```
aws ec2 describe-images --executable-users self
```

Exemplo: Listar AMIs de propriedade da Amazon

O comando a seguir lista as AMIs de propriedade da Amazon. As AMIs públicas da Amazon têm um proprietário com alias, que aparece como `amazon` no campo da conta. Isso permite que você encontre AMIs da Amazon facilmente. Outros usuários não podem dar um alias às AMIs deles.

```
aws ec2 describe-images --owners amazon
```

Exemplo: Listar AMIs de propriedade de uma conta

O comando a seguir lista as AMIs de propriedade da conta AWS específica.

```
aws ec2 describe-images --owners 123456789012
```

Exemplo: Definir escopo das AMIs usando um filtro

Para reduzir o número de AMIs exibidas, use um filtro para listar somente os tipos de AMI que lhe interessam. Por exemplo, use o filtro a seguir para exibir somente AMIs com EBS.

```
--filters "Name=root-device-type,Values=ebs"
```

Tornar um AMI pública

O Amazon EC2 permite que você compartilhe suas AMIs com outras contas da AWS. Você pode permitir que todas as contas AWS usem a AMI para executar instâncias (tornando a AMI pública) ou apenas permitir que algumas contas específicas usem a AMI para executar instâncias (consulte [Compartilhar uma AMI com contas específicas da AWS \(p. 112\)](#)). Você não é cobrado quando sua AMI é usada por outras contas AWS para executar instâncias; somente as instâncias que são executadas usando a AMI são cobradas pelas instâncias executadas.

Não é possível tornar AMIs com volumes criptografados públicos.

As AMIs são um recurso regional. Portanto, compartilhar uma AMI a disponibiliza nessa região. Para disponibilizar uma AMI em uma região diferente, copie a AMI para a região e compartilhe-a. Para obter mais informações, consulte [Copiar um AMI \(p. 120\)](#).

Se uma AMI tiver um código de produto ou contiver um snapshot de um volume criptografado, você não poderá torná-la pública; você poderá compartilhar a AMI somente com contas específicas da AWS.

Tópicos

- [Compartilhar uma AMI com todas as contas da AWS \(console\) \(p. 111\)](#)
- [Compartilhar uma AMI com todas as contas da AWS \(Tools for Windows PowerShell\) \(p. 111\)](#)
- [Compartilhar uma AMI com todas as contas da AWS \(AWS CLI\) \(p. 112\)](#)

Compartilhar uma AMI com todas as contas da AWS (console)

Depois de tornar uma AMI pública, ela estará disponível em AMIs da comunidade ao executar uma instância na mesma região usando o console. Observe que pode demorar um pouco para a AMI aparecer em AMIs da comunidade depois de você torná-la pública. Pode também demorar um pouco para a AMI ser removida das AMIs da comunidade quando você torná-la novamente privada.

Para compartilhar uma AMI pública usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione AMIs.
3. Selecione sua AMI na lista e escolha Ações, Modificar permissões de imagens.
4. Escolha Pública e Salvar.

Compartilhar uma AMI com todas as contas da AWS (Tools for Windows PowerShell)

Cada AMI tem uma propriedade `launchPermission` que controla quais contas da AWS, além da do proprietário, têm permissão para usar essa AMI para executar instâncias. Ao modificar a propriedade `launchPermission` da AMI, você pode torná-la pública (o que concede permissões de execução a todas as contas da AWS) ou compartilhá-la somente com as contas da AWS que especificar.

Você pode adicionar ou remover os IDs da lista de contas que tiverem permissões de execução para uma AMI. Para tornar a AMI pública, especifique o grupo `all`. Você pode especificar permissões públicas e permissões de execução explícita.

Para tornar um AMI pública

1. Use o comando `Edit-EC2ImageAttribute` da seguinte forma para adicionar o grupo `all` à lista `launchPermission` para a AMI especificada.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute launchPermission -OperationType add -UserGroup all
```

2. Para verificar as permissões de execução das AMIs, use o comando `Get-EC2ImageAttribute`.

```
PS C:\> Get-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute launchPermission
```

3. (Opcional) Para tornar a AMI privada novamente, remova o grupo `all` de suas permissões de execução. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute launchPermission -OperationType remove -UserGroup all
```

Compartilhar uma AMI com todas as contas da AWS (AWS CLI)

Cada AMI tem uma propriedade `launchPermission` que controla quais contas da AWS, além da do proprietário, têm permissão para usar essa AMI para executar instâncias. Ao modificar a propriedade `launchPermission` da AMI, você pode torná-la pública (o que concede permissões de execução a todas as contas da AWS) ou compartilhá-la somente com as contas da AWS que especificar.

Você pode adicionar ou remover os IDs da lista de contas que tiverem permissões de execução para uma AMI. Para tornar a AMI pública, especifique o grupo `all`. Você pode especificar permissões públicas e permissões de execução explícita.

Para tornar um AMI pública

1. Use o comando [modify-image-attribute](#) da forma a seguir para adicionar o grupo `all` à lista `launchPermission` para a AMI especificada.

```
aws ec2 modify-image-attribute \
--image-id ami-0abcdef1234567890 \
--launch-permission "Add=[{Group=all}]"
```

2. Para verificar as permissões de execução da AMI, use o comando [describe-image-attribute](#).

```
aws ec2 describe-image-attribute \
--image-id ami-0abcdef1234567890 \
--attribute launchPermission
```

3. (Opcional) Para tornar a AMI privada novamente, remova o grupo `all` de suas permissões de execução. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando.

```
aws ec2 modify-image-attribute \
--image-id ami-0abcdef1234567890 \
--launch-permission "Remove=[{Group=all}]"
```

Compartilhar uma AMI com contas específicas da AWS

Você pode compartilhar uma AMI com contas específicas da AWS sem torná-la pública. Tudo de que você precisa são os IDs de conta da AWS. Só é possível compartilhar AMIs que tenham volumes não criptografados e volumes criptografados com uma chave gerenciada pelo cliente. Se você compartilhar uma AMI com volumes criptografados, também deverá compartilhar todas as chaves gerenciadas pelo cliente usadas para criptografá-los. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#). Não é possível compartilhar uma AMI que tenha volumes criptografados com uma Chave gerenciada pela AWS .

As AMIs são um recurso regional. Portanto, compartilhar uma AMI a disponibiliza nessa região. Para disponibilizar uma AMI em uma região diferente, copie a AMI para a região e compartilhe-a. Para obter mais informações, consulte [Copiar um AMI \(p. 120\)](#).

Não há limite para o número de contas da AWS com as quais uma AMI pode ser compartilhada. As tags definidas pelo usuário anexadas a uma AMI compartilhada estão disponíveis somente na sua conta da AWS e não nas outras contas com as quais a AMI é compartilhada.

Compartilhar uma AMI (console)

Para conceder permissões de execução explícita usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione AMIs.
3. Selecione sua AMI na lista e escolha Ações, Modificar permissões de imagens.
4. Especifique o número da conta da AWS do usuário com quem você deseja compartilhar a AMI no campo Número de conta da AWS e selecione Adicionar permissão.

Para compartilhar essa AMI com múltiplos usuários, repita essa etapa até adicionar todos os usuários necessários.

Note

Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Só a AMI em si precisa ser compartilhada; o sistema fornece automaticamente acesso à instância dos snapshots do Amazon EBS referenciados para a execução. No entanto, você precisa compartilhar todas as Chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#).

5. Escolha Save (Salvar) quando terminar.
6. (Opcional) Para visualizar os IDs de conta da AWS com que você compartilhou a AMI, selecione a AMI na lista e escolha a guia Permissions (Permissões). Para localizar as AMIs que são compartilhadas com você, consulte [Encontrar AMIs compartilhadas \(p. 108\)](#).

Compartilhar uma AMI (Tools for Windows PowerShell)

Use o comando `Edit-EC2ImageAttribute` (Tools for Windows PowerShell) para compartilhar uma AMI conforme exibido nos exemplos a seguir.

Para conceder permissões de execução explícitas

O comando a seguir concede permissões de execução da AMI especificada para a conta da AWS especificada.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute launchPermission - OperationType add -UserId "123456789012"
```

Note

Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Só a AMI em si precisa ser compartilhada; o sistema fornece automaticamente acesso à instância dos snapshots do Amazon EBS referenciados para a execução. No entanto, você precisa compartilhar todas as Chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#).

Para remover as permissões de execução de uma conta

O comando a seguir remove permissões de execução para a AMI especificada da conta especificada da AWS:

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute launchPermission - OperationType remove -UserId "123456789012"
```

Para remover todas as permissões de execução

O comando a seguir remove todas as permissões de execução explícita e pública da AMI especificada. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute launchPermission
```

Compartilhar uma AMI (AWS CLI)

Use o comando [modify-image-attribute](#) (AWS CLI) para compartilhar uma AMI conforme exibido nos exemplos a seguir.

Para conceder permissões de execução explícitas

O comando a seguir concede permissões de execução da AMI especificada para a conta da AWS especificada.

```
aws ec2 modify-image-attribute \  
--image-id ami-0abcdef1234567890 \  
--launch-permission "Add=[{UserId=123456789012}]"
```

Note

Você não precisa compartilhar os snapshots do Amazon EBS aos quais a AMI faz referência para compartilhar a AMI. Só a AMI em si precisa ser compartilhada; o sistema fornece automaticamente acesso à instância dos snapshots do Amazon EBS referenciados para a execução. No entanto, você precisa compartilhar todas as Chaves do KMS usadas para criptografar os snapshots referenciados pela AMI. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#).

Para remover as permissões de execução de uma conta

O comando a seguir remove permissões de execução para a AMI especificada da conta especificada da AWS:

```
aws ec2 modify-image-attribute \  
--image-id ami-0abcdef1234567890 \  
--launch-permission "Remove=[{UserId=123456789012}]"
```

Para remover todas as permissões de execução

O comando a seguir remove todas as permissões de execução explícita e pública da AMI especificada. Observe que o proprietário da AMI sempre tem permissões de execução e, portanto, não é afetado por este comando.

```
aws ec2 reset-image-attribute \  
--image-id ami-0abcdef1234567890 \  
--attribute launchPermission
```

Usar marcadores

Se você tiver criado uma AMI pública ou compartilhado uma AMI com outro usuário da AWS, pode criar um favorito que permita ao usuário acessar sua AMI e executar uma instância em sua própria conta

imediatamente. Essa é uma maneira fácil de compartilhar referências de AMI, de forma que os usuários não tenham de gastar tempo para encontrar sua AMI para utilizá-la.

Observe que sua AMI deve ser pública; caso contrário, você deve tê-la compartilhado com o usuário a quem deseja enviar o favorito.

Para criar um favorito para sua AMI

1. Digite um URL com as informações a seguir, onde região é a região na qual sua AMI reside:

```
https://console.aws.amazon.com/ec2/v2/home?  
region=region#LaunchInstanceWizard:ami=ami_id
```

Por exemplo, esse URL executa uma instância a partir da AMI 0abcdef1234567890 na região us-east-1:

```
https://console.aws.amazon.com/ec2/v2/home?region=us-  
east-1#LaunchInstanceWizard:ami=ami-0abcdef1234567890
```

2. Distribua o link para os usuários que desejam usar sua AMI.
3. Para usar um favorito, escolha o link ou copie-o e cole-o no navegador. O assistente de execução se abre com as AMIs já selecionadas.

Melhores práticas para AMIs compartilhadas do Windows

Use as diretrizes a seguir para reduzir a superfície de ataque e melhorar a confiabilidade das AMIs criadas.

- Nenhuma lista de diretrizes de segurança consegue ser exaustiva. Crie suas AMIs compartilhadas cuidadosamente e tire um tempo para considerar onde você pode expor dados confidenciais.
- Desenvolva um processo repetível para criar, atualizar e republicar as AMIs.
- Crie AMIs usando os sistemas operacionais, pacotes e softwares mais atualizados.
- [Faça download](#) e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte [Instalar a versão mais recente do EC2Config \(p. 532\)](#).
- Verifique se Ec2SetPassword, Ec2WindowsActivate e Ec2HandleUserData estão habilitados.
- Verifique se não estão presentes nenhuma conta de convidado ou contas de usuários de Desktop Remoto.
- Desabilite ou remova os serviços e programas desnecessários para reduzir a superfície de ataque da sua AMI.
- Elimine as credenciais da instância, como o par de chaves, da AMI (se você tiver gravado na AMI). Armazene as credenciais em um local seguro.
- Certifique-se de que a senha do administrador e as senhas de todas as outras contas estão definidas a um valor apropriado para compartilhar. Essas senhas estão disponíveis para qualquer pessoa que execute sua AMI compartilhada.
- Teste sua AMI antes de compartilhá-la.

AMIs pagas

Após criar uma AMI, você pode mantê-la privada para que somente você possa usá-la ou pode compartilhá-la com uma lista especificada de contas da AWS. Você também pode tornar pública sua AMI personalizada para que a comunidade possa usá-la. A criação de uma AMI segura, protegida e utilizável

para consumo público é um processo bastante direto, quando você segue algumas diretrizes simples. Para obter informações sobre como criar e usar AMIs compartilhadas, consulte [AMIs compartilhadas \(p. 108\)](#).

Você pode comprar AMIs de terceiros, incluindo AMIs fornecidas com contratos de serviço de organizações como a Red Hat. Você também pode criar uma AMI e vendê-la para outros usuários do Amazon EC2.

AMI paga é uma AMI que você pode comprar de um desenvolvedor.

O Amazon EC2 integra-se ao AWS Marketplace , permitindo aos desenvolvedores cobrem outros usuários do Amazon EC2 pelo uso de AMIs ou fornecer suporte para instâncias.

O AWS Marketplace é uma loja online na qual você pode adquirir o software executado na AWS, incluindo as AMIs usadas na execução da instância do EC2. As AMIs do AWS Marketplace são organizadas em categorias, como Ferramentas para desenvolvedores, o que permite que você encontre produtos para atender às suas necessidades. Para obter mais informações sobre o AWS Marketplace , consulte o site [AWS Marketplace](#) .

Executar uma instância de uma AMI paga é o mesmo que executar uma instância de qualquer outra AMI. Nenhum parâmetro adicional é necessário. A instância é cobrada de acordo com as taxas definidas pelo proprietário da AMI, bem como as taxas de uso padrão dos serviços Web relacionados; por exemplo, a taxa por hora para execução de um tipo de instância m1.small no Amazon EC2. Taxas adicionais também podem ser cobradas. O proprietário da AMI paga pode confirmar se uma determinada instância foi executada usando essa AMI paga.

Important

O Amazon DevPay não está mais aceitando novos vendedores ou produtos. O AWS Marketplace agora é a única plataforma unificada de comércio eletrônico para vender software e serviços por meio da AWS. Para obter informações sobre como implantar e vender software do AWS Marketplace , consulte [Como vender no AWS Marketplace](#). O AWS Marketplace oferece suporte para AMIs com o Amazon EBS.

Tópicos

- [Vender sua AMI \(p. 116\)](#)
- [Localizar uma AMI paga \(p. 116\)](#)
- [Comprar uma AMI paga \(p. 118\)](#)
- [Obter o código do produto para sua instância \(p. 118\)](#)
- [Usar suporte pago \(p. 118\)](#)
- [Faturas para AMI pagas e compatíveis \(p. 119\)](#)
- [Gerenciar suas assinaturas do AWS Marketplace \(p. 119\)](#)

Vender sua AMI

Você pode vender a AMI usando o AWS Marketplace . O AWS Marketplace oferece uma experiência de compras organizada. Além disso, o AWS Marketplace também oferece suporte a recursos da AWS, como AMIs baseadas em Amazon EBS, instâncias reservadas e instâncias spot.

Para obter informações sobre como vender a AMI no AWS Marketplace , consulte [Como vender no AWS Marketplace](#).

Localizar uma AMI paga

Há algumas formas de encontrar AMIs que estão disponíveis para compra. Por exemplo, você pode usar o [AWS Marketplace](#) , o console do Amazon EC2 ou a linha de comando. De forma alternativa, um desenvolvedor pode, por conta própria, informar você sobre uma AMI paga.

Para localizar uma AMI paga usando o console

Para localizar uma AMI paga usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione AMIs.
3. No primeiro filtro, escolha Imagens públicas.
4. Na barra Search (Pesquisar), escolha Owner (Proprietário) e, em seguida, AWS Marketplace .
5. Se você souber o código do produto, escolha Product Code e digite o código do produto.

Localizar uma AMI paga usando o AWS Marketplace

Para encontrar uma AMI paga usando o AWS Marketplace

1. Aberto [AWS Marketplace](#) .
2. Digite o nome do sistema operacional na caixa de pesquisa e clique em Ir.
3. Para definir ainda mais o escopo dos resultados, use uma das categorias ou filtros.
4. Cada produto é identificado com o tipo: **AMI** ou **Software as a Service**.

Localizar uma AMI paga usando o Tools for Windows PowerShell

Você pode encontrar uma AMI paga usando o seguinte comando [Get-EC2Image](#).

```
PS C:\> Get-EC2Image -Owner aws-marketplace
```

A saída de uma AMI paga inclui o código do produto.

ProductCodeId	ProductCodeType
----- <i>product_code</i>	----- marketplace

Se você souber o código do produto, poderá filtrar os resultados por código do produto. Esse exemplo retorna a AMI mais recente com o código do produto especificado.

```
PS C:\> (Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-code"; "Value"="product_code"} | sort CreationDate -Descending | Select-Object -First 1).ImageId
```

Localizar uma AMI paga usando o AWS CLI

Você pode encontrar uma AMI paga usando o seguinte comando [describe-images](#) (AWS CLI).

```
aws ec2 describe-images  
--owners aws-marketplace
```

Esse comando retorna detalhes numerosos que descrevem cada AMI, incluindo o código do produto para uma AMI paga. A saída de `describe-images` inclui uma entrada para o código do produto como o seguinte:

```
"ProductCodes": [  
 {
```

```
        "ProductCodeId": "product_code",  
        "ProductCodeType": "marketplace"  
    },  
],
```

Se você souber o código do produto, poderá filtrar os resultados por código do produto. Esse exemplo retorna a AMI mais recente com o código do produto especificado.

```
aws ec2 describe-images  
  --owners aws-marketplace \  
  --filters "Name=product-code,Values=product_code" \  
  --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

Comprar uma AMI paga

Você deve cadastrar-se (para comprar) uma AMI paga para poder executar uma instância usando a AMI.

Normalmente, um vendedor de uma AMI paga apresenta informações sobre as AMIs, incluindo o preço e um link no qual você pode comprá-las. Quando você clicar no link, será solicitado que você faça login na AWS e, em seguida, você poderá comprar a AMI.

Comprar uma AMI paga usando o console

Você pode comprar uma AMI paga usando o assistente de execução do Amazon EC2. Para obter mais informações, consulte [Executar uma instância AWS Marketplace \(p. 441\)](#).

Assinar um produto usando o AWS Marketplace

Para usar o AWS Marketplace, você deve ter uma conta da AWS. Para executar instâncias de produtos do AWS Marketplace, você deve estar cadastrado para usar o serviço Amazon EC2 e ter assinado o produto do qual executar a instância. Há duas maneiras de assinar produtos no AWS Marketplace :

- Site do AWS Marketplace : você pode executar o software pré-configurado rapidamente com o recurso de implantação de um clique.
- Assistente de execução do Amazon EC2: você pode procurar uma AMI e executar uma instância diretamente do assistente. Para obter mais informações, consulte [Executar uma instância AWS Marketplace \(p. 441\)](#).

Obter o código do produto para sua instância

Recupere o código do produto do AWS Marketplace para sua instância usando os metadados da instância. Para obter mais informações sobre como recuperar os metadados, consulte [Metadados da instância e dados do usuário \(p. 622\)](#).

Para recuperar um código do produto, use o comando a seguir:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/product-codes
```

Se a instância tiver um código de produto, o Amazon EC2 o retornará.

Usar suporte pago

O Amazon EC2 também permite que desenvolvedores ofereçam suporte para o software (ou AMI derivadas). Os desenvolvedores podem criar produtos de suporte nos quais você pode se cadastrar para

usar. Durante o cadastro no produto de suporte, o desenvolvedor oferece a você um código de produto, que você deve associar à sua própria AMI. Isso permite ao desenvolvedor confirmar que sua instância está qualificada para suporte. Também garante que quando você executar instâncias do produto, você será cobrado de acordo com os termos do produto especificado pelo desenvolvedor.

Important

Você não pode usar um produto de suporte com Instâncias reservadas. Você sempre paga o preço que está especificado pelo vendedor do produto de suporte.

Para associar um código de produto com sua AMI, use um dos seguintes comandos, em que `ami_id` é o ID da AMI e `product_code` é o código do produto:

- [modify-image-attribute](#) (AWS CLI)

```
aws ec2 modify-image-attribute --image-id ami_id --product-codes "product_code"
```

- [Edit-EC2ImageAttribute](#) (AWS Tools for Windows PowerShell)

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami_id -ProductCode product_code
```

Depois de definir o atributo de código de produto, ele não pode ser alterado nem removido.

Faturas para AMI pagas e compatíveis

No final de cada mês, você recebe um e-mail com o valor que foi cobrado de seu cartão de crédito pelo uso de todas as AMIs pagas ou compatíveis durante o mês. Essa conta é separada de sua conta normal do Amazon EC2. Para obter mais informações, consulte [Pagamento de produtos](#) no Guia do comprador do AWS Marketplace .

Gerenciar suas assinaturas do AWS Marketplace

No site do AWS Marketplace , você pode verificar os detalhes de sua assinatura, visualizar as instruções de uso do fornecedor, gerenciar as assinaturas, etc.

Para verificar os detalhes de sua assinatura

1. Faça login no [AWS Marketplace](#) .
2. Escolha Your Marketplace Account.
3. Escolha Manage your software subscriptions.
4. Todas as assinaturas atuais estão listadas. Escolha Usage Instructions para exibir instruções específicas sobre o uso do produto; por exemplo, um nome de usuário para se conectar à instância em execução.

Para cancelar a assinatura do AWS Marketplace

1. Certifique-se de que você tenha encerrado todas as instâncias em execução da assinatura.
 - a. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
 - b. No painel de navegação, escolha Instances (Instâncias).
 - c. Selecione a instância e escolha Actions, Instance State e Terminate.
 - d. Quando a confirmação for solicitada, escolha Sim, encerrar.
2. Inicie a sessão no [AWS Marketplace](#) , escolha Your Marketplace Account (Sua conta do Marketplace) e, depois, Manage your software subscriptions (Gerenciar suas assinaturas de software).

3. Escolha Cancel subscription. Será solicitada a confirmação do cancelamento.

Note

Depois de cancelar sua assinatura, você não poderá mais executar nenhuma instância dessa AMI. Para usar essa AMI novamente, você precisará assiná-la novamente, no site do AWS Marketplace ou através do Launch Wizard no console do Amazon EC2.

Ciclo de vida da AMI

Tópicos

- [Criar uma AMI \(p. 120\)](#)
- [Copiar um AMI \(p. 120\)](#)
- [Armazenar e restaurar uma AMI usando o S3 \(p. 126\)](#)
- [Defasjar uma AMI \(p. 132\)](#)
- [Automatizar o ciclo de vida da AMI com suporte do EBS \(p. 135\)](#)

Criar uma AMI

Para obter informações sobre como criar uma AMI do Windows, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#).

Para obter informações sobre como criar uma AMI, consulte [Criar uma AMI do Linux baseada em Amazon EBS](#) ou [Criar uma AMI em Linux com armazenamento de instâncias](#).

Copiar um AMI

Você pode copiar uma imagem de máquina da Amazon (AMI) dentro ou através de Regiões AWS. Você pode copiar as AMIs baseadas no Amazon EBS e as AMIs com armazenamento de instâncias. Você pode copiar AMIs com snapshots criptografados e também alterar o status de criptografia durante o processo de cópia. Você pode copiar as AMIs que são compartilhadas com você.

Copiar uma AMI de origem resulta em uma AMI de destino idêntica, mas com seu próprio identificador exclusivo. Você pode alterar ou cancelar o registro da AMI de origem sem afetar a AMI de destino. O inverso também é verdadeiro.

No caso de uma AMI baseada no Amazon EBS, cada um de seus snapshots de suporte é, copiado para um snapshot de destino idêntico, mas distinto. Se você copiar uma AMI para uma nova Região, os snapshots serão cópias completas (não incrementais). Se você criptografar snapshots de suporte não criptografados ou criptografá-los para uma nova chave KMS, os snapshots serão cópias completas (não incrementais). Operações de cópia subsequentes de uma AMI resultam em cópias incrementais dos snapshots de suporte.

Não há cobrança para copiar uma AMI. Mas aplicam-se as taxas padrão de transferência de dados e armazenamento. Se copiar uma AMI baseada em EBS, você será cobrado pelo armazenamento de snapshots adicionais do EBS.

Considerations

- Você pode usar políticas do IAM para conceder ou negar permissões de usuários para copiar AMIs. As permissões no nível do recurso especificadas para a ação `CopyImage` se aplicam somente à nova AMI. Não é possível especificar permissões no nível do recurso para a AMI de origem.
- A AWS não copia permissões de execução, tags definidas pelo usuário nem permissões do bucket do Amazon S3 da AMI de origem para a nova AMI. Após a conclusão da operação de cópia, você poderá

aplicar permissões de execução, tags definidas pelo usuário e permissões do bucket do Amazon S3 à nova AMI.

- Se você estiver usando uma AMI do AWS Marketplace ou uma AMI derivada diretamente ou indiretamente de uma AMI do AWS Marketplace , não será possível copiá-la entre contas. Em vez disso, execute uma instância do EC2 usando a AMI do AWS Marketplace e crie uma AMI a partir da instância. Para obter mais informações, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#) .

Tópicos

- [Permissões para copiar uma AMI com armazenamento de instâncias \(p. 121\)](#)
- [Copiar um AMI \(p. 122\)](#)
- [Parar uma operação de cópia de AMI pendente \(p. 123\)](#)
- [Cópia entre regiões \(p. 123\)](#)
- [Cópia entre contas \(p. 124\)](#)
- [Criptografar e copiar \(p. 125\)](#)

Permissões para copiar uma AMI com armazenamento de instâncias

Se você usar um usuário do IAM para copiar uma AMI com armazenamento de instâncias, o usuário deverá ter as seguintes permissões do Amazon S3: s3>CreateBucket, s3:GetBucketAcl, s3>ListAllMyBuckets, s3GetObject, s3:PutObject e s3:PutObjectAcl.

A política de exemplo a seguir permite que o usuário copie a origem de AMI no bucket especificado para a região especificada.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "s3>ListAllMyBuckets",  
            "Resource": [  
                "arn:aws:s3:::*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": "s3GetObject",  
            "Resource": [  
                "arn:aws:s3:::ami-source-bucket/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3>CreateBucket",  
                "s3:GetBucketAcl",  
                "s3:PutObjectAcl",  
                "s3:PutObject"  
            ],  
            "Resource": [  
                "arn:aws:s3:::amis-for-123456789012-in-us-east-1*"  
            ]  
        }  
    ]  
}
```

Para localizar o nome do recurso da Amazon (ARN) do bucket de origem da AMI, abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2>. No painel de navegação, escolha AMIs e localize o nome do bucket na coluna Source (Origem).

Note

A permissão `s3:CreateBucket` é necessária somente na primeira vez em que o usuário do IAM copia uma AMI com armazenamento de instâncias para uma região individual. Depois disso, o bucket do Amazon S3 que foi criado na região será usado para armazenar todas as AMIs futuras que você copiar para essa região.

Copiar um AMI

Você pode copiar uma AMI usando AWS Management Console, AWS Command Line Interface ou SDKs, ou a API do Amazon EC2, que dão suporte à ação `CopyImage`.

Prerequisite

Crie ou obtenha uma AMI com um snapshot do Amazon EBS. Observe que você pode usar o console do Amazon EC2 para pesquisar por uma grande variedade de AMIs fornecidas pela AWS. Para obter mais informações, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#) e [Localizar uma AMI](#).

Para copiar uma AMI usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Pela barra de navegação do console, selecione a região que contém a AMI. No painel de navegação, selecione Images (Imagens), AMIs para exibir a lista de AMIs disponíveis para você na região.
3. Selecione a AMI para copiar e escolha Actions (Ações), Copy AMI (Copiar AMI).
4. Na caixa de diálogo Copy AMI (Copiar AMI), especifique as seguintes informações e escolha Copy AMI (Copiar AMI):
 - Destination region (Região de destino): a região para a qual a AMI deve ser copiada. Para obter mais informações, consulte [Cópia entre regiões \(p. 123\)](#).
 - Name (Nome): o nome da nova AMI. Você pode incluir informações do sistema operacional no nome, pois não fornecemos essas informações ao exibir detalhes sobre a AMI.
 - Description (Descrição): por padrão, a descrição inclui informações sobre a AMI de origem, de forma que você possa distinguir uma cópia da original. Você pode alterar essa descrição conforme necessário.
 - Encryption (Criptografia): selecione este campo para criptografar snapshots de destino ou recriptográfi-los usando uma chave diferente. Se você tiver ativado a [criptografia por padrão \(p. 1426\)](#), a opção Encryption (Criptografia) será configurada e não poderá ser desconfigurada no console do snapshot. Para obter mais informações, consulte [Criptografar e copiar \(p. 125\)](#).
 - Chave do KMS: a chave do KMS usada para criptografar os snapshots de destino.
5. Nós exibimos uma página de confirmação para avisá-lo que a operação de cópia foi iniciada e fornecer a você o ID da nova AMI.

Para verificar imediatamente o progresso da operação de cópia, siga o link fornecido. Para verificar o progresso depois, escolha Done (Concluído) e, quando você estiver pronto, use a barra de navegação para alternar para a região de destino (se aplicável) e localize sua AMI na lista de AMIs.

O status inicial da AMI de destino é `pending` e a operação será concluída quando o status for `available`.

Para copiar uma AMI usando a AWS CLI

Você pode copiar uma AMI usando o comando [copy-image](#). Você deve especificar as regiões de origem e de destino. Especifique a região de origem usando o parâmetro `--source-region`. Você pode especificar a região de destino usando o parâmetro `--region` ou uma variável de ambiente. Para obter mais informações, consulte [Configurar a interface de linha de comando da AWS](#).

Quando você criptografa um snapshot de destino durante a cópia, deve especificar os parâmetros adicionais: `--encrypted` e `--kms-key-id`.

Para copiar uma AMI usando a Tools for Windows PowerShell

Você pode copiar uma AMI usando o comando [Copy-EC2Image](#). Você deve especificar as regiões de origem e de destino. Especifique a região de origem usando o parâmetro `-SourceRegion`. Você pode especificar a região de destino usando o parâmetro `-Region` ou o comando `Set-AWSDefaultRegion`. Para obter mais informações, consulte [Especificação das regiões da AWS](#).

Quando você criptografa um snapshot de destino durante a cópia, deve especificar os parâmetros adicionais: `-Encrypted` e `-KmsKeyId`.

Parar uma operação de cópia de AMI pendente

Você pode parar uma cópia de AMI pendente da forma a seguir.

Para parar uma operação de cópia de AMI usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região de destino com o seletor de região.
3. No painel de navegação, selecione AMIs.
4. Selecione a AMI cuja cópia será interrompida e escolha Actions (Ações) e Deregister (Cancelar registro).
5. Quando solicitada confirmação, selecione Continue (Continuar).

Para parar uma operação de cópia de AMI usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [deregister-image](#) (AWS CLI)
- [Unregister-EC2Image](#) (AWS Tools for Windows PowerShell)

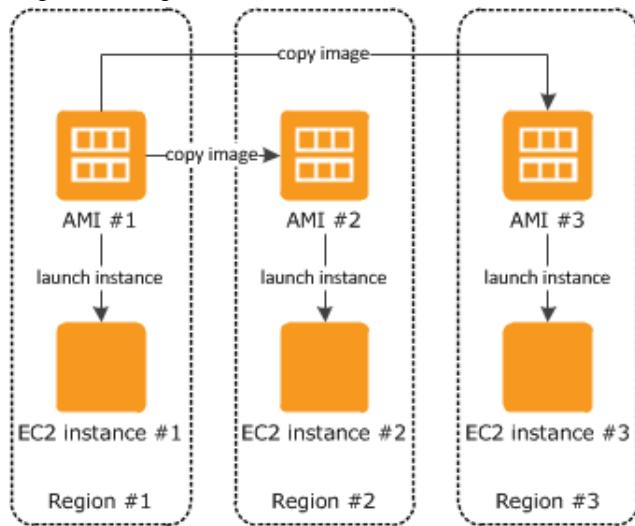
Cópia entre regiões

Copiar uma AMI entre regiões geograficamente diversas traz os seguintes benefícios:

- **Implantação global consistente:** copiar uma AMI de uma região para outra permite que você execute instâncias consistentes com base na mesma AMI em diferentes regiões.
- **Escalabilidade:** Você pode mais facilmente projetar e construir aplicações globais que atendam às necessidades dos seus usuários, onde quer que estejam.
- **Performance:** você pode aumentar a performance ao distribuir sua aplicação, além de localizar os componentes essenciais da sua aplicação em maior proximidade de seus usuários. Você também pode aproveitar recursos específicos da região, como tipos de instância ou outros serviços da AWS.
- **Alta disponibilidade:** você pode projetar e implantar aplicações nas regiões da AWS, de forma a aumentar a disponibilidade.

O diagrama a seguir mostra as relações entre uma AMI de origem e duas AMIs copiadas em regiões diferentes, assim como as instâncias do EC2 executadas de cada uma. Ao executar uma instância a partir

de uma AMI, ela residirá na mesma região em que a AMI reside. Se você fizer alterações à AMI de origem e quiser que essas alterações sejam refletidas nas AMIs das regiões de destino, deve recopiar a AMI de origem nas regiões de destino.



Ao copiar pela primeira vez uma AMI com armazenamento de instâncias para uma região, criaremos um bucket do Amazon S3 para as AMIs copiadas para essa região. Todas as AMIs com armazenamento de instâncias que você copiar para essa região serão armazenadas nesse bucket. Os nomes do bucket têm o seguinte formato: `amis-for-account-in-region-hash`. Por exemplo: `amis-for-123456789012-in-us-east-2-yhjmxvp6`.

Prerequisite

Antes de copiar uma AMI, é preciso garantir que o conteúdo da AMI de origem seja atualizado para oferecer suporte à execução em uma região diferente. Por exemplo, você deve atualizar todas as strings de conexão com o banco de dados ou dados de configuração de aplicação para apontarem para os recursos apropriados. Caso contrário, as instâncias executadas pela nova AMI na região de destino ainda poderão usar os recursos da região de origem, o que pode afetar a performance e o custo.

Limits

- As regiões de destino estão limitadas a 100 cópias simultâneas de AMI.

Cópia entre contas

É possível compartilhar uma AMI com outra conta da AWS. O compartilhamento da AMI não afeta propriedade da AMI. A conta proprietária é cobrada pelo armazenamento na região. Para obter mais informações, consulte [Compartilhar uma AMI com contas específicas da AWS \(p. 112\)](#).

Se você copiar uma AMI que foi compartilhada com sua conta, será o proprietário da AMI de destino na sua conta. Do proprietário da AMI de origem são cobradas taxas de transferência padrão do Amazon EBS ou do Amazon S3, e você será cobrado pelo armazenamento da AMI de destino na região de destino.

Permissões de recursos

Para copiar uma AMI compartilhada com você por outra conta, o proprietário da AMI de origem deve conceder permissão de leitura para armazenamento que suporta a AMI, seus snapshots EBS associados (para uma AMI com Amazon EBS) ou um bucket S3 associado (para uma AMI com armazenamento de instâncias). Se a AMI compartilhada criptografou snapshots, o proprietário deve compartilhar a chave ou as chaves com você também.

Criptografar e copiar

A tabela a seguir mostra o suporte a criptografia para vários cenários de cópia de AMI. Apesar de ser possível copiar um snapshot não criptografado para render um snapshot criptografado, você não pode copiar um snapshot criptografado para render um não criptografado.

Cenário	Descrição	Compatível
1	Não criptografado para não criptografado	Sim
2	Criptografado para criptografado	Sim
3	Não criptografado para criptografado	Sim
4	Criptografado para não criptografado	Não

Note

A criptografia durante a ação `CopyImage` se aplica somente a AMIs com Amazon EBS. Como uma AMI com armazenamento de instâncias não depende de snapshots, você não pode usar a cópia para alterar seu status de criptografia.

Por padrão (isto é, sem especificar parâmetros de criptografia), o snapshot de suporte de uma AMI é copiado com seu status de criptografia original. Copiar uma AMI baseada em um snapshot não criptografado resulta em um snapshot de destino idêntico que também não é criptografado. Se a AMI de origem da for baseada em um snapshot criptografado, copiá-la resultará em um snapshot de destino idêntico que é criptografado pela mesma chave do AWS KMS. Copiar uma AMI com vários snapshots preserva, por padrão, o status de criptografia de origem em cada snapshot de destino.

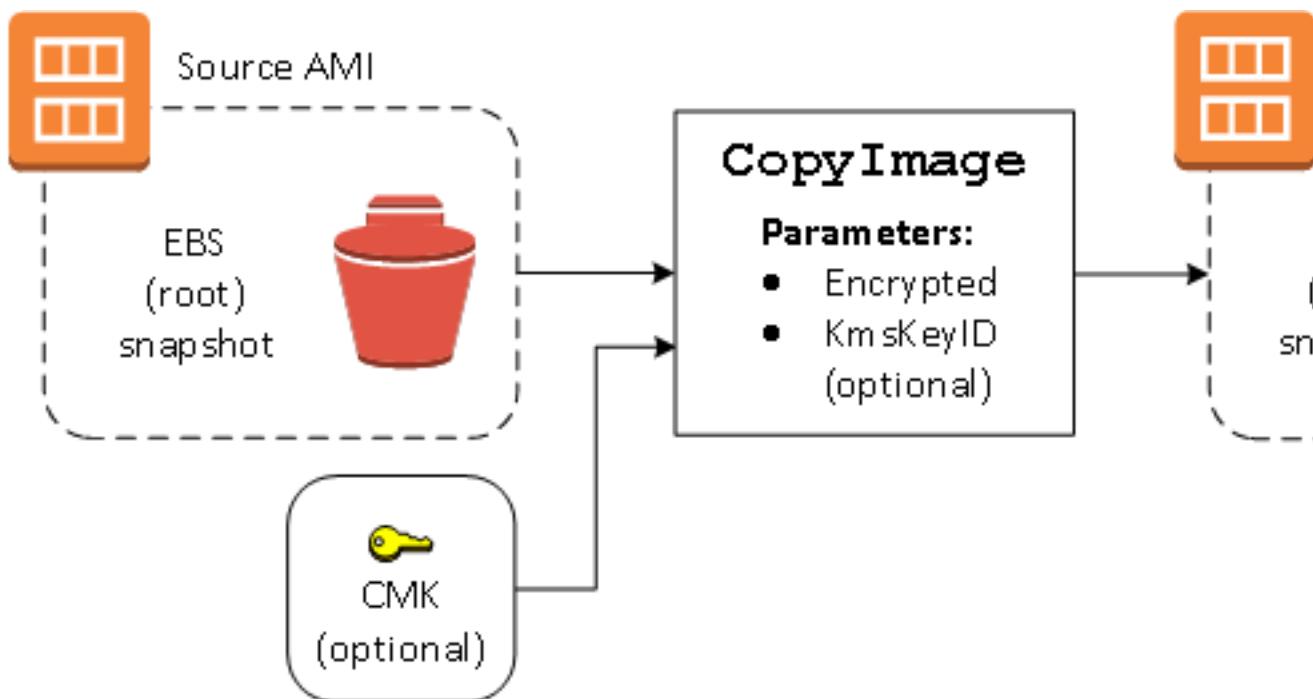
Se você especificar parâmetros de criptografia enquanto copia uma AMI, poderá criptografar seus snapshots de suporte ou criptografá-los novamente. O exemplo a seguir mostra um caso não padrão que fornece parâmetros de criptografia à ação `CopyImage` para alterar o estado de criptografia da AMI de destino.

Copiar uma AMI de origem não criptografada para uma AMI de destino criptografada

Nesse cenário, uma AMI baseada em um snapshot raiz não criptografado é copiada para uma AMI com um snapshot raiz criptografado. A ação `CopyImage` é invocada com dois parâmetros de criptografia, incluindo uma chave gerenciada pelo cliente. Como resultado, o status de criptografia do snapshot raiz muda, de modo que a AMI de destino tenha suporte de um snapshot raiz contendo os mesmos dados que o snapshot de origem, mas criptografado usando a chave especificada. Você incorre em custos de armazenamento para os snapshots em ambas as AMIs, bem como cobranças para todas as instâncias iniciadas a partir de uma AMI.

Note

Habilitar a [Criptografia por padrão](#) (p. 1426) tem o mesmo efeito que configurar o parâmetro `Encrypted` como `true` para todos os snapshots na AMI.



Configurar o parâmetro `Encrypted` criptografa o snapshot único dessa instância. Se você não especificar o parâmetro `KmsKeyId`, a chave gerenciada pelo cliente padrão será usada para criptografar a cópia do snapshot.

Para obter mais informações sobre como copiar AMIs com snapshots criptografados, consulte [Usar criptografia com AMIs com EBS \(p. 135\)](#).

Armazenar e restaurar uma AMI usando o S3

Você pode armazenar uma imagem de máquina da Amazon (AMI) em um bucket do Amazon S3, copiar a AMI para outro bucket do S3 e restaurá-la a partir do bucket do S3. Ao armazenar e restaurar uma AMI usando buckets do S3, você pode copiar AMIs de uma partição da AWS para outra, por exemplo, da principal partição comercial para a partição AWS GovCloud (US) . Você também pode fazer cópias de arquivamento de AMIs armazenando-as em um bucket do S3.

As APIs compatíveis para armazenar e restaurar uma AMI usando o S3 são `CreateStoreImageTask`, `DescribeStoreImageTasks` e `CreateRestoreImageTask`.

`CopyImage` é a API recomendada para copiar AMIs dentro de uma [partição](#) da AWS. No entanto, `CopyImage` não pode copiar uma AMI para outra partição.

Warning

Certifique-se de cumprir todas as leis e requisitos de negócios aplicáveis ao mover dados entre partções da AWS ou regiões da AWS, incluindo, entre outros, quaisquer regulamentos governamentais aplicáveis e requisitos de residência de dados.

Tópicos

- [Casos de uso \(p. 127\)](#)
- [Como as APIs de armazenamento e restauração da AMI funcionam \(p. 128\)](#)
- [Limitations \(p. 129\)](#)
- [Costs \(p. 129\)](#)

- [Proteger suas AMIs \(p. 130\)](#)
- [Permissões para armazenar e restaurar AMIs usando o S3 \(p. 130\)](#)
- [Trabalhar com o armazenamento da AMI e restaurar APIs \(p. 131\)](#)

Casos de uso

Use as APIs de armazenamento e restauração para fazer o seguinte:

- [Copiar uma AMI de uma partição da AWS para outra partição da AWS \(p. 127\)](#)
- [Fazer cópias de arquivamento de AMIs \(p. 127\)](#)

Copiar uma AMI de uma partição da AWS para outra partição da AWS

Ao armazenar e restaurar uma AMI usando buckets do S3, você pode copiar uma AMI de uma partição da AWS para outra ou de uma região da AWS para outra. No exemplo a seguir, você copia uma AMI da partição comercial principal para a partição AWS GovCloud (US) , especificamente da região us-east-2 para a região us-gov-east-1.

Para copiar uma AMI de uma partição para outra, siga estas etapas:

- Armazene a AMI em um bucket do S3 na região atual usando `CreateStoreImageTask`. Neste exemplo, o bucket do S3 está localizado em us-east-2. Para obter um exemplo de comando, consulte [Armazenar uma AMI em um bucket do S3 \(p. 131\)](#).
- Monitore o andamento da tarefa de armazenamento usando `DescribeStoreImageTasks`. O objeto fica visível no bucket do S3 quando a tarefa é concluída. Para obter um exemplo de comando, consulte [Descrever o andamento de uma tarefa de armazenamento de AMI \(p. 131\)](#).
- Copie o objeto da AMI armazenado para um bucket do S3 na partição de destino usando um procedimento de sua escolha. Neste exemplo, o bucket do S3 está localizado em us-gov-east-1.

Note

Como você precisa de credenciais diferentes da AWS para cada partição, você não pode copiar um objeto S3 diretamente de uma partição para outra. O processo para copiar um objeto S3 entre partções está fora do escopo desta documentação. Fornecemos os processos de cópia a seguir como exemplos, mas você deve usar o processo de cópia que atenda aos seus requisitos de segurança.

- Para copiar uma AMI entre partções, o processo de cópia pode ser tão simples quanto o seguinte: [Faça o download do objeto](#) do bucket de origem para um host intermediário (por exemplo, uma instância do EC2 ou um laptop) e, em seguida, [faça upload do objeto](#) do host intermediário no bucket de origem. Para cada etapa do processo, use as credenciais da AWS para a partição.
- Para um uso mais sustentável, considere desenvolver uma aplicação que gerencia as cópias, potencialmente usando [downloads e uploads de várias partes](#) do S3.
- Restaure a AMI do bucket do S3 na partição de destino usando `CreateRestoreImageTask`. Neste exemplo, o bucket do S3 está localizado em us-gov-east-1. Para obter um exemplo de comando, consulte [Restaurar uma AMI de um bucket do S3 \(p. 131\)](#).
- Monitore o andamento da tarefa de restauração descrevendo a AMI para verificar quando seu estado se torna disponível. Você também pode monitorar as porcentagens de progresso dos snapshots que compõem a AMI restaurada descrevendo os instantâneos.

Fazer cópias de arquivamento de AMIs

Você pode fazer cópias de arquivamento de AMIs armazenando-as em um bucket do S3. Para obter um exemplo de comando, consulte [Armazenar uma AMI em um bucket do S3 \(p. 131\)](#).

A AMI é embalada em um único objeto no S3 e todos os metadados da AMI (excluindo informações de compartilhamento) são preservados como parte da AMI armazenada. Os dados da AMI são compactados como parte do processo de armazenamento. AMIs que contêm dados que podem ser facilmente compactados resultarão em objetos menores no S3. Para reduzir custos, você pode usar camadas de armazenamento S3 mais econômicas. Para obter mais informações, consulte [Classes de armazenamento do Amazon S3](#) e [definição de preço do Amazon S3](#)

Como as APIs de armazenamento e restauração da AMI funcionam

Para armazenar e restaurar uma AMI usando o S3, use as seguintes APIs:

- [CreateStoreImageTask](#) – Armazena a AMI em um bucket do S3
- [DescribeStoreImageTasks](#) – Fornece o andamento da tarefa de armazenamento da AMI
- [CreateRestoreImageTask](#) – Restaura a AMI de um bucket do S3

Como as APIs funcionam

- [CreateStoreImageTask \(p. 128\)](#)
- [DescribeStoreImageTasks \(p. 128\)](#)
- [CreateRestoreImageTask \(p. 129\)](#)

CreateStoreImageTask

A API [CreateStoreImageTask \(p. 131\)](#) armazena uma AMI como um único objeto em um bucket do S3.

A API cria uma tarefa que lê todos os dados da AMI e seus snapshots e, a seguir, usa um [multipart upload do S3](#) para armazenar os dados em um objeto do S3. A API leva todos os componentes da AMI, incluindo a maioria dos metadados de AMI não específicos da região e todos os snapshots do EBS contidos na AMI, e os empacota em um único objeto no S3. Os dados são compactados como parte do processo de upload para reduzir a quantidade de espaço usado no S3; portanto, o objeto no S3 pode ser menor do que a soma dos tamanhos dos snapshots na AMI.

Se houver tags de AMI e de snapshot visíveis para a conta chamando essa API, elas serão preservadas.

O objeto no S3 tem o mesmo ID que a AMI, mas com uma extensão .bin. Os dados a seguir também são armazenados como tags de metadados do S3 no objeto do S3: nome da AMI, descrição da AMI, data de registro da AMI, conta de proprietário da AMI e um timestamp para a operação de armazenamento.

O tempo necessário para concluir a tarefa depende do tamanho da AMI. Também depende de quantas outras tarefas estão em andamento porque as tarefas estão em fila. Você pode acompanhar o andamento da tarefa chamando a API [DescribeStoreImageTasks \(p. 131\)](#).

A soma dos tamanhos de todas as AMIs em andamento é limitada a 600 GB de dados de snapshot do EBS por conta. A criação de tarefas adicionais será rejeitada até que as tarefas em andamento sejam inferiores ao limite. Por exemplo, se uma AMI com 100 GB de dados de snapshot e outra AMI com 200 GB de dados de snapshot estiverem sendo armazenadas no momento, outra solicitação será aceita, pois o total em andamento é de 300 GB, que é inferior ao limite. Mas se uma única AMI com 800 GB de dados de snapshot estiver sendo armazenada no momento, outras tarefas serão rejeitadas até que a tarefa seja concluída.

DescribeStoreImageTasks

A API [DescribeStoreImageTasks \(p. 131\)](#) descreve o andamento das tarefas de armazenamento da AMI. Você pode descrever tarefas para AMIs especificadas. Se você não especificar AMIs, receberá uma lista paginada de todas as tarefas de imagem de armazenamento que foram processadas nos últimos 31 dias.

Para cada tarefa de AMI, a resposta indica se a tarefa é `InProgressCompleted` ou `Failed`. Para tarefas `InProgress`, a resposta mostra um andamento estimado como uma porcentagem.

As tarefas são listadas em ordem cronológica inversa.

No momento, somente as tarefas do mês anterior podem ser visualizadas.

CreateRestoreImageTask

A API [CreateRestoreImageAsk \(p. 131\)](#) inicia uma tarefa que restaura uma AMI de um objeto do S3 que foi criado anteriormente usando uma solicitação [CreateStoreImageAsk \(p. 131\)](#).

A tarefa de restauração pode ser executada na mesma região ou em uma região diferente daquela em que a tarefa de armazenamento foi executada.

O bucket do S3 a partir do qual o objeto da AMI será restaurado deve estar na mesma região em que a tarefa de restauração é solicitada. A AMI será restaurada nessa região.

A AMI é restaurada com seus metadados, como o nome, a descrição e os mapeamentos de dispositivos de blocos correspondentes aos valores da AMI armazenada. O nome deve ser exclusivo para AMIs na região dessa conta. Se você não fornecer um nome, a nova AMI obterá o mesmo nome da AMI original. A AMI obtém um novo ID de AMI que é gerado no momento do processo de restauração.

O tempo necessário para a conclusão da tarefa de restauração da AMI depende do tamanho da AMI. Também depende de quantas outras tarefas estão em andamento porque as tarefas estão em fila. Você pode visualizar o andamento da tarefa descrevendo a AMI ([describe-images](#)) ou seus snapshots do EBS ([describe-snapshots](#)). Se a tarefa falhar, a AMI e os snapshots serão movidos para um estado com falha.

A soma dos tamanhos de todas as AMIs em andamento é limitada a 300 GB (com base no tamanho após a restauração) dos dados de snapshot do EBS por conta. A criação de tarefas adicionais será rejeitada até que as tarefas em andamento sejam inferiores ao limite.

Limitations

- Somente AMIs baseadas no EBS podem ser armazenadas usando essas APIs.
- AMIs paravirtuais (PV) não são suportadas.
- O tamanho de uma AMI (antes da compactação) que pode ser armazenada é limitado ao limite de tamanho de um único objeto do S3, que é de 1 TB.
- Cota em solicitações de [imagem de armazenamento \(p. 131\)](#) : 600 GB de trabalho de armazenamento (dados de snapshots) em andamento.
- Cota em solicitações de [imagem de restauração \(p. 131\)](#) : 300 GB de trabalho de restauração (dados de snapshots) em andamento.
- Durante a tarefa de armazenamento, os snapshots não devem ser excluídos e a entidade principal do IAM que faz o armazenamento deve ter acesso aos snapshots, caso contrário o processo de armazenamento apresentará falha.
- Não é possível criar várias cópias de uma AMI no mesmo bucket do S3.
- Uma AMI armazenada em um bucket do S3 não pode ser restaurada com seu ID de AMI original. Você pode mitigar isso usando [Alias de AMI](#).
- Atualmente, as APIs de armazenamento e restauração só são compatíveis se for utilizada a AWS Command Line Interface, os AWS SDKs e a API do Amazon EC2. Não é possível armazenar e restaurar uma AMI usando o console do Amazon EC2.

Costs

Quando você armazena e restaura AMIs usando o S3, é cobrado pelos serviços usados pelas APIs de armazenamento e restauração e pela transferência de dados. As APIs usam o S3 e a API direta do EBS

(usadas internamente por essas APIs para acessar os dados do snapshot). Para obter mais informações, consulte [Definição de preço do Amazon S3](#) e [Definição de preço do Amazon EBS](#).

Proteger suas AMIs

Para usar as APIs de armazenamento e restauração, o bucket do S3 e a AMI devem estar na mesma região. É importante garantir que o bucket do S3 esteja configurado com segurança suficiente para proteger o conteúdo da AMI e que a segurança seja mantida enquanto os objetos da AMI permanecerem no bucket. Se isso não puder ser feito, o uso dessas APIs não será recomendado. Não permita acesso público ao bucket do S3. Recomendamos que você ative a [Server Side Encryption](#) (Criptografia do lado do servidor) para o bucket do S3 no qual você armazena as AMIs, embora não seja necessário.

Para obter informações sobre como definir as configurações de segurança apropriadas para os buckets do S3, consulte os seguintes tópicos de segurança:

- [Bloquear o acesso público ao armazenamento do Amazon S3](#)
- [Definir o comportamento padrão da criptografia para os buckets do Amazon S3](#)
- [Qual política de bucket do S3 eu devo usar para aderir à regra s3-bucket-ssl-requests-only do AWS Config?](#)
- [Habilitar o log de acesso ao servidor do Amazon S3](#)

Quando os snapshots da AMI são copiados para o objeto S3, os dados são copiados em conexões TLS. Você pode armazenar AMIs com snapshots criptografados, mas os snapshots são descriptografados como parte do processo de armazenamento.

Permissões para armazenar e restaurar AMIs usando o S3

Caso as entidades principais do IAM armazenem ou restaurem AMIs usando o S3, você precisará conceder a elas as permissões necessárias.

A política de exemplo a seguir inclui todas as ações necessárias para permitir que uma entidade principal do IAM execute as tarefas de armazenamento e restauração.

Você também pode criar políticas para que as entidades principais do IAM só possam acessar recursos nomeados. Para obter mais exemplos de políticas, consulte [Gerenciamento de acesso para recursos daAWS](#) no Guia do usuário do IAM.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3:DeleteObject",  
                "s3:GetObject",  
                "s3>ListBucket",  
                "s3:PutObject",  
                "s3:AbortMultipartUpload",  
                "ebs:CompleteSnapshot",  
                "ebs:GetSnapshotBlock",  
                "ebs>ListChangedBlocks",  
                "ebs>ListSnapshotBlocks",  
                "ebs:PutSnapshotBlock",  
                "ebs:StartSnapshot",  
                "ec2>CreateStoreImageTask",  
                "ec2:DescribeStoreImageTasks",  
                "ec2>CreateRestoreImageTask",  
                "ec2:GetEbsEncryptionByDefault",  
                "ec2:DescribeTags"  
            ]  
        }  
    ]  
}
```

```
        ],
        "Resource": "*"
    }
}
```

Trabalhar com o armazenamento da AMI e restaurar APIs

Tópicos

- [Armazenar uma AMI em um bucket do S3 \(p. 131\)](#)
- [Descrever o andamento de uma tarefa de armazenamento de AMI \(p. 131\)](#)
- [Restaurar uma AMI de um bucket do S3 \(p. 131\)](#)

Armazenar uma AMI em um bucket do S3

Para armazenar uma AMI (AWS CLI)

Use o comando [create-store-image-task](#). Especifique o ID da AMI e o nome do bucket do S3 no qual a AMI será armazenada.

```
aws ec2 create-store-image-task \
--image-id ami-1234567890abcdef0 \
--bucket myamibucket
```

Saída esperada

```
{
    "ObjectKey": "ami-1234567890abcdef0.bin"
}
```

Descrever o andamento de uma tarefa de armazenamento de AMI

Para descrever o andamento de uma tarefa de armazenamento de AMI (AWS CLI)

Use o comando [describe-store-image-tasks](#).

```
aws ec2 describe-store-image-tasks
```

Saída esperada

```
{
    "AmiId": "ami-1234567890abcdef0",
    "Bucket": "myamibucket",
    "ProgressPercentage": 17,
    "S3ObjectKey": "ami-1234567890abcdef0.bin",
    "StoreTaskState": "InProgress",
    "StoreTaskFailureReason": null,
    "TaskStartTime": "2021-01-01T01:01:01.001Z"
}
```

Restaurar uma AMI de um bucket do S3

Para restaurar uma AMI (AWS CLI)

Use o comando [create-restore-image-task](#). Usando os valores de `S3ObjectKey` e `Bucket` da `describe-store-image-tasks` saída, especifique a chave de objeto da AMI e o nome do bucket do S3 para o qual

a AMI foi copiada. Especifique também um nome para a AMI restaurada. O nome deve ser exclusivo para AMIs na região dessa conta.

Note

A AMI restaurada obtém um novo ID de AMI.

```
aws ec2 create-restore-image-task \
--object-key ami-1234567890abcdef0.bin \
--bucket myamibucket \
--name "New AMI Name"
```

Saída esperada

```
{  
    "ImageId": "ami-0eab20fe36f83e1a8"  
}
```

Defasar uma AMI

É possível defasar uma AMI para indicar que ela está desatualizada e não deve ser usada. Também é possível especificar uma data de defasagem futura para uma AMI, indicando quando a AMI estará desatualizada. Por exemplo, você pode defasar uma AMI cuja manutenção não está mais ativa ou pode defasar uma AMI que foi substituída por uma versão mais recente. Por padrão, as AMIs defasadas não aparecem nas listagens de AMI, impedindo que novos usuários usem AMIs desatualizadas. No entanto, os usuários existentes e os serviços de inicialização, como modelos de inicialização e grupos do Auto Scaling, podem continuar usando uma AMI defasada especificando seu ID. Para excluir a AMI, de modo que usuários e serviços não possam usá-la, é necessário [cancelar o registro](#) (p. 55) dela.

Depois que uma AMI estiver defasada:

- Para usuários de AMI, a AMI defasada não aparece nas chamadas de API [DescribeImages](#), a menos que você especifique o ID dela ou especifique que AMIs defasadas devem ser exibidas. Os proprietários da AMI continuam a ver AMIs defasadas nas chamadas de API [DescribeImages](#).
- Para usuários de AMI, a AMI defasada não está disponível para seleção no console do EC2. Por exemplo, uma AMI defasada não é exibida no catálogo da AMI no assistente de inicialização de instância. Os proprietários da AMI continuam a ver AMIs defasadas no console do EC2.
- Para os usuários da AMI, se você souber o ID de uma AMI defasada, poderá continuar a iniciar instâncias usando a AMI defasada com a API, a CLI ou os SDKs.
- Os serviços de inicialização, como modelos de inicialização e grupos do Auto Scaling, podem continuar referenciando a AMIs defasadas.
- As instâncias do EC2 que foram iniciadas usando uma AMI que posteriormente é defasada não são afetadas e podem ser interrompidas, iniciadas e reinicializadas.

Você pode defasar AMIs privadas e públicas.

Você também pode criar políticas de AMI apoiadas pelo EBS Amazon Data Lifecycle Manager para automatizar a defasagem das AMIs apoiadas pelo EBS. Para obter mais informações, consulte [Automatizar ciclos de vida da AMI](#) (p. 1376).

Tópicos

- [Costs](#) (p. 133)
- [Limitations](#) (p. 129)
- [Defasar uma AMI](#) (p. 133)
- [Descrever AMIs defasadas](#) (p. 133)

- [Cancelar a defasagem de uma AMI \(p. 135\)](#)

Costs

Quando você defasar uma AMI, a AMI não será excluída. O proprietário da AMI continuará pagando pelos snapshots da AMI. Para parar de pagar pelos instantâneos, o proprietário da AMI deve excluir a AMI [cancelando o registro \(p. 55\)](#) dela.

Limitations

- Para defasar uma AMI, é necessário ser o proprietário da AMI.
- Não é possível usar o console do EC2 para defasar uma AMI ou cancelar a defasagem de uma AMI.

Defasar uma AMI

Você pode defasar uma AMI em uma data e hora específicas. É necessário ser o proprietário da AMI para executar esse procedimento.

Para defasar uma AMI em uma data específica (AWS CLI)

Usar o comando [disable-image-deprecation](#). Especifique o ID da AMI e a data e hora nas quais a AMI será defasada. Se você especificar um valor para segundos, o Amazon EC2 arredondará os segundos para o minuto mais próximo.

```
aws ec2 enable-image-deprecation \
  --image-id ami-1234567890abcdef0 \
  --deprecate-at "2021-10-15T13:17:12.000Z"
```

Saída esperada

```
{  
  "RequestID": "59dbff89-35bd-4eac-99ed-be587EXAMPLE",  
  "Return": "true"  
}
```

Descrever AMIs defasadas

Quando você descreve todas as AMIs usando o comando [describe-images](#), os resultados são diferentes, dependendo se você é usuário da AMI ou proprietário da AMI.

- Se você for um usuário da AMI:

Por padrão, quando você descreve todas as AMIs usando o comando [describe-images](#), as AMIs defasadas das quais você não é proprietário, mas que são compartilhadas com você, não são exibidas nos resultados. Para incluir AMIs defasadas nos resultados, é necessário especificar o parâmetro `--include-deprecated true`. O valor padrão para `--include-deprecated` é `false`. Se você omitir esse parâmetro, as AMIs defasadas não serão exibidas nos resultados.

- Se você for o proprietário da AMI:

Quando você descreve todas as AMIs usando o comando [describe-images](#), todas as AMIs das quais você é proprietário, inclusive AMIs defasadas, são exibidas nos resultados. Não é necessário especificar o parâmetro `--include-deprecated true`. Além disso, não é possível excluir AMIs defasadas que você possui dos resultados usando `--include-deprecated false`.

Se uma AMI estiver defasada, o campo `DeprecationTime` é exibido nos resultados.

Note

Uma AMI defasada é uma AMI cuja data de defasagem já passou. Se você tiver definido a data de defasagem como uma data futura, a AMI ainda não está defasada.

Para incluir todas as AMIs defasada ao descrever todas as AMIs (AWS CLI)

Use o comando [describe-images](#) e especifique o parâmetro `--include-deprecated` com um valor de `true` para incluir nos resultados todas as AMIs defasadas das quais você não é proprietário.

```
aws ec2 describe-images \
--region us-east-1 \
--owners 123456example
--include-deprecated true
```

Para descrever a data de defasagem de uma AMI (AWS CLI)

Use o comando [describe-images](#) e especifique o ID da AMI.

Se você especificar `--include-deprecated false` com o ID da AMI, os resultados retornarão a AMI defasada.

```
aws ec2 describe-images \
--region us-east-1 \
--image-ids ami-1234567890EXAMPLE
```

Saída esperada

O campo `DeprecationTime` exibe a data definida para a defasagem da AMI. Se não houver data para a defasagem da AMI não estiver definida, o campo `DeprecationTime` não será exibido na saída.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "available",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2021-05-10T13:17:12.000Z",
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "LastModified": "2019-05-10T13:17:12.000Z"
        }
    ]
}
```

```
        "Public": true,  
        "ImageType": "machine",  
        "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"  
    }  
}  
}
```

Cancelar a defasagem de uma AMI

É possível cancelar a defasagem de uma AMI, que remove o campo `DeprecationTime` da saída [describe-images](#). É necessário ser o proprietário da AMI para executar esse procedimento.

Para cancelar a defasagem de uma AMI (AWS CLI)

Use o comando `disable-image-deprecation` e especifique o ID da AMI.

```
aws ec2 disable-image-deprecation \  
  --image-id ami-1234567890abcdef0
```

Saída esperada

```
{  
  "RequestID": "11aabb229-4eac-35bd-99ed-be587EXAMPLE",  
  "Return": "true"  
}
```

Automatizar o ciclo de vida da AMI com suporte do EBS

Você pode usar Amazon Data Lifecycle Manager para automatizar a criação, a retenção, a cópia, a defasagem e a exclusão de AMIs baseadas no Amazon EBS e seus snapshots de backup. Para obter mais informações, consulte [Amazon Data Lifecycle Manager \(p. 1363\)](#).

Usar criptografia com AMIs com EBS

As AMIs com snapshots do Amazon EBS podem se beneficiar da criptografia do Amazon EBS. Os snapshots de volumes raiz e de dados podem ser criptografados e anexados a uma AMI. Você pode executar instâncias e copiar imagens com suporte total à criptografia do EBS. Os parâmetros de criptografia para essas operações são compatíveis em todas as regiões em que o AWS KMS está disponível.

As instâncias do EC2 com volumes do EBS criptografados são executadas em AMIs da mesma forma que outras instâncias. Além disso, ao executar uma instância a partir de uma AMI baseada em snapshots não criptografados do EBS, você poderá criptografar alguns ou todos os volumes durante a execução.

Como os volumes do EBS, os snapshots em AMIs podem ser criptografados pelo padrão Chave do AWS KMS key ou por um chave gerenciada pelo cliente que você especificar. Em todos os casos, você deve ter permissão para usar a Chave do KMS selecionada.

As AMIs com snapshots criptografados podem ser compartilhadas em todas as contas da AWS. Para obter mais informações, consulte [AMIs compartilhadas \(p. 108\)](#).

Tópicos de criptografia em AMIs com EBS

- [Cenários de execução de instância \(p. 136\)](#)
- [Cenários de cópia de imagem \(p. 138\)](#)

Cenários de execução de instância

As instâncias do Amazon EC2 são executadas a partir de AMIs usando a ação `RunInstances` com parâmetros fornecidos pelo mapeamento de dispositivos de blocos, seja por meio do AWS Management Console ou diretamente usando a CLI ou a API do Amazon EC2. Para obter mais informações sobre o mapeamento de dispositivos de blocos, consulte [Mapeamento de dispositivos de blocos](#). Para exemplos de mapeamento de dispositivos de blocos da AWS CLI, consulte [Executar, listar e encerrar instâncias do EC2](#).

Por padrão, sem parâmetros de criptografia explícitos, uma ação `RunInstances` mantém o estado de criptografia existente dos snapshots de origem de uma AMI enquanto restaura os volumes do EBS a partir deles. Se a [Criptografia por padrão \(p. 1426\)](#) estiver habilitada, todos os volumes criados a partir da AMI (seja de snapshots criptografados ou não criptografados) serão criptografados. Se a criptografia por padrão não estiver habilitada, a instância manterá o estado de criptografia da AMI.

Você também pode executar uma instância e aplicar simultaneamente um estado de criptografia aos volumes resultantes fornecendo parâmetros de criptografia. Consequentemente, os seguintes comportamentos são observados:

Executar sem parâmetros de criptografia

- Um snapshot não criptografado é restaurado para um volume não criptografado, a menos que a criptografia por padrão esteja habilitada, e, nesse caso, todos os volumes recém-criados serão criptografados.
- Um snapshot criptografado que você possui é restaurado para um volume que é criptografado para a mesma Chave do KMS.
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é restaurado para um volume que é criptografado pela chave do KMS padrão da sua conta da AWS.

Os comportamentos padrão podem ser substituídos fornecendo parâmetros de criptografia. Os parâmetros disponíveis são `Encrypted` e `KmsKeyId`. Configurar somente o parâmetro `Encrypted` resulta no seguinte:

A instância executa comportamentos com `Encrypted` definido, mas sem `KmsKeyId` especificado

- Um snapshot não criptografado é restaurado para um volume do EBS que é criptografado pela chave do KMS padrão da sua conta da AWS.
- Um snapshot criptografado que você possui é restaurado para um volume do EBS criptografado pela mesma Chave do KMS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é restaurado para um volume que é criptografado pela chave do KMS padrão da sua conta da AWS. (Em outras palavras, o parâmetro `Encrypted` não tem efeito.)

A configuração dos parâmetros `Encrypted` e `KmsKeyId` permite especificar uma Chave do KMS não padrão para uma operação de criptografia. Os seguintes comportamentos resultam em:

A instância com `Encrypted` e `KmsKeyId` definidos

- Um snapshot não criptografado é restaurado para um volume do EBS criptografado pela Chave do KMS especificada.
- Um snapshot criptografado é restaurado para um volume do EBS criptografado, não para a Chave do KMS original, mas para a Chave do KMS especificada.

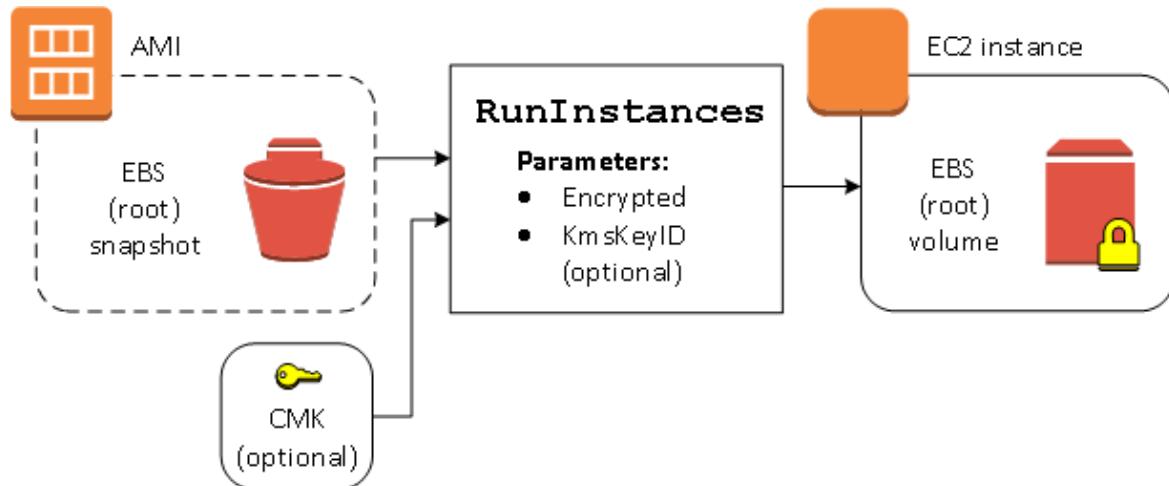
Enviar um `KmsKeyId` sem também configurar o parâmetro `Encrypted` resulta em um erro.

As seções a seguir fornecem exemplos da execução de instâncias de AMIs usando parâmetros de criptografia não padrão. Em cada um desses cenários, os parâmetros fornecidos à ação `RunInstances` resultam em uma alteração do estado de criptografia durante a restauração de um volume a partir de um snapshot.

Para obter informações sobre como usar o console para executar uma instância a partir de uma AMI, consulte [Executar sua instância \(p. 417\)](#).

Criptografar um volume durante a execução

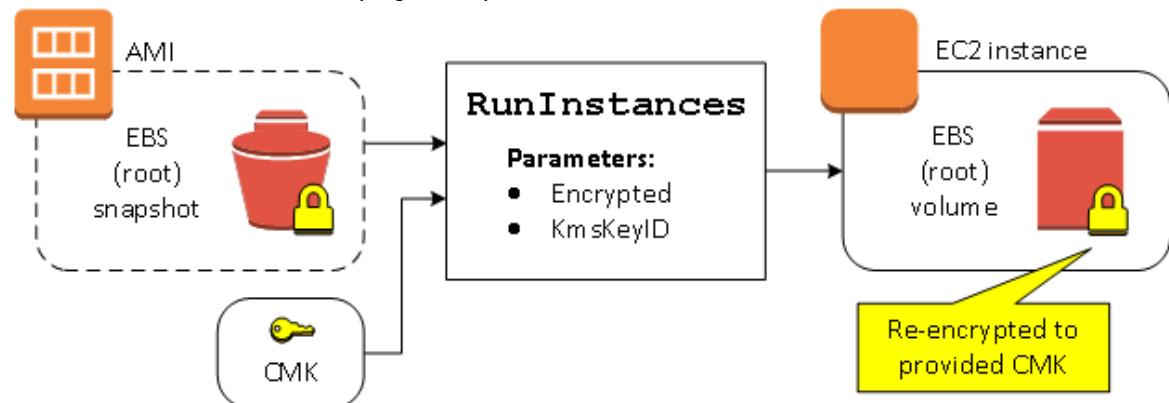
Neste exemplo, uma AMI baseada em um snapshot não criptografado é usada para executar uma instância do EC2 com um volume não criptografado do EBS.



Somente o parâmetro `Encrypted` resulta no volume que será criptografado para essa instância. É opcional fornecer um parâmetro `KmsKeyId`. Se nenhum ID de Chave do KMS for especificado, a Chave do KMS padrão da conta da AWS será usada para criptografar o volume. Para criptografar o volume em uma Chave do KMS diferente que pertença a você, forneça o parâmetro `KmsKeyId`.

Criptografar novamente um volume durante a execução

Neste exemplo, uma AMI baseada em um snapshot criptografado é usada para executar uma instância do EC2 com um volume do EBS criptografado por uma nova Chave do KMS.

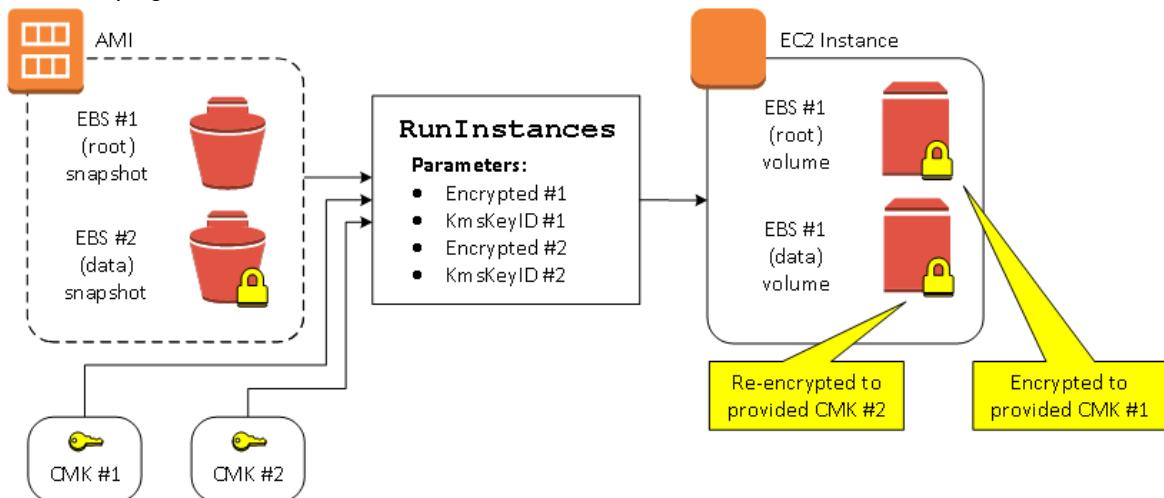


Se você possuir a AMI e não fornecer nenhum parâmetro de criptografia, a instância resultante terá um volume criptografado pela mesma Chave do KMS do snapshot. Se a AMI for compartilhada e não pertencer a você, e nenhum parâmetro de criptografia for fornecido, o volume será criptografado pela

Chave do KMS padrão. Com os parâmetros de criptografia fornecidos conforme mostrado, o volume será criptografado pela Chave do KMS especificada.

Alterar o estado de criptografia de vários volumes durante a execução

Neste exemplo mais complexo, uma AMI baseada em vários snapshots (cada um com seu próprio estado de criptografia) é usada para executar uma instância do EC2 com um volume recém-criptografado e um volume criptografado novamente.



Neste cenário, a ação `RunInstances` é fornecida com parâmetros de criptografia para cada um dos snapshots de origem. Quando todos os parâmetros possíveis de criptografia forem especificados, a instância resultante será a mesma, independentemente de você possuir a AMI.

Cenários de cópia de imagem

As AMIs do Amazon EC2 são copiadas usando a ação `CopyImage`, seja pelo AWS Management Console ou diretamente usando a CLI ou a API do Amazon EC2.

Por padrão, sem parâmetros de criptografia explícitos, uma ação `CopyImage` mantém o estado de criptografia existente dos snapshots de origem de uma AMI durante a cópia. Você também pode copiar uma AMI e aplicar simultaneamente um novo estado de criptografia aos snapshots associados do EBS fornecendo parâmetros de criptografia. Consequentemente, os seguintes comportamentos são observados:

Copiar sem parâmetros de criptografia

- Um snapshot não criptografado é copiado para outro snapshot não criptografado, a menos que a criptografia por padrão esteja habilitada, e, nesse caso, todos os snapshots recém-criados serão criptografados.
- Um snapshot criptografado de sua propriedade é copiado para um snapshot criptografado com a mesma Chave do KMS.
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é copiado para um snapshot que é criptografado pela chave do KMS padrão da sua conta da AWS.

Todos esses comportamentos padrão podem ser substituídos fornecendo parâmetros de criptografia. Os parâmetros disponíveis são `Encrypted` e `KmsKeyId`. Configurar somente o parâmetro `Encrypted` resulta no seguinte:

Comportamentos de cópia de imagem com **Encrypted** definido, mas nenhum **KmsKeyId** especificado

- Um snapshot não criptografado é copiado para um snapshot criptografado pela chave do KMS padrão da conta da AWS.
- Um snapshot criptografado é copiado para outro snapshot criptografado pela mesma Chave do KMS. (Em outras palavras, o parâmetro **Encrypted** não tem efeito.)
- Um snapshot criptografado do qual você não é proprietário (por exemplo, a AMI é compartilhada com você) é copiado para um volume que é criptografado pela chave do KMS padrão da sua conta da AWS. (Em outras palavras, o parâmetro **Encrypted** não tem efeito.)

A configuração dos parâmetros **Encrypted** e **KmsKeyId** permite especificar uma Chave do KMS gerenciada pelo cliente para uma operação de criptografia. Os seguintes comportamentos resultam em:

Comportamentos de cópia de imagem com **Encrypted** e **KmsKeyId** definidos

- Um snapshot não criptografado é copiado para um snapshot criptografado pela Chave do KMS especificada.
- Um snapshot criptografado é copiado para outro snapshot criptografado, não para a Chave do KMS original, mas para a Chave do KMS especificada.

Enviar um **KmsKeyId** sem também configurar o parâmetro **Encrypted** resulta em um erro.

A seção a seguir fornece um exemplo de como copiar uma AMI usando parâmetros de criptografia não padrão, resultando em uma alteração do estado de criptografia.

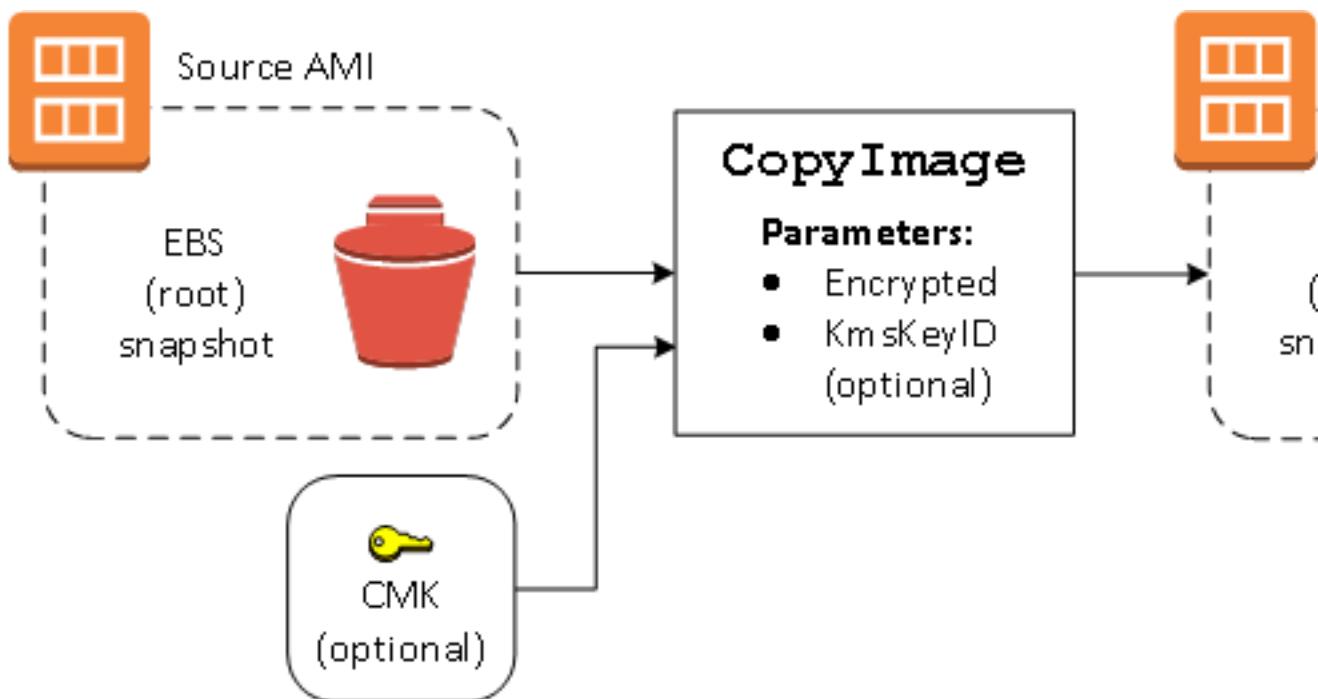
Para obter instruções detalhadas usando o console, consulte [Copiar um AMI \(p. 120\)](#).

Criptografar uma imagem não criptografada durante a cópia

Nesse cenário, uma AMI baseada em um snapshot raiz não criptografado é copiada para uma AMI com um snapshot raiz criptografado. A ação `CopyImage` é invocada com dois parâmetros de criptografia, incluindo uma chave gerenciada pelo cliente. Como resultado, o status de criptografia do snapshot raiz muda, de modo que a AMI de destino tenha suporte de um snapshot raiz contendo os mesmos dados que o snapshot de origem, mas criptografado usando a chave especificada. Você incorre em custos de armazenamento para os snapshots em ambas as AMIs, bem como cobranças para todas as instâncias iniciadas a partir de uma AMI.

Note

Habilitar a [Criptografia por padrão \(p. 1426\)](#) tem o mesmo efeito que configurar o parâmetro **Encrypted** como `true` para todos os snapshots na AMI.



Configurar o parâmetro `Encrypted` criptografa o snapshot único dessa instância. Se você não especificar o parâmetro `KmsKeyId`, a chave gerenciada pelo cliente padrão será usada para criptografar a cópia do snapshot.

Note

Você também pode copiar uma imagem com vários snapshots e configurar o estado de criptografia de cada uma individualmente.

Noções básicas sobre as informações de faturamento da AMI

Há muitas Imagens de máquina da Amazon (AMIs) para escolher ao executar suas instâncias e elas oferecem suporte a uma variedade de plataformas e recursos do sistema operacional. Para entender como a AMI escolhida ao executar sua instância afeta os resultados da sua fatura da AWS, você pode pesquisar a plataforma do sistema operacional associada e as informações de faturamento. Faça isso antes de executar qualquer on-demand ou Instâncias spot, ou comprar uma Instância reservada.

Aqui estão dois exemplos de como pesquisar sua AMI com antecedência pode ajudá-lo a escolher a AMI que melhor se adapte às suas necessidades:

- Para Instâncias spot, você pode usar os detalhes da plataforma da AMI para confirmar se a AMI é suportada para Instâncias spot.
- Ao comprar uma Instância reservada, você pode certificar-se de selecionar a plataforma do sistema operacional (Plataforma) que mapeia para os detalhes da PlataformaAMI.

Para obter mais informações sobre a definição de instâncias, consulte [Definição de preço do Amazon EC2](#).

Tópicos

- [Campos de informações de faturamento da AMI \(p. 141\)](#)

- Localizando detalhes de faturamento e uso da AMI (p. 142)
- Verificar cobranças da AMI em sua fatura (p. 144)

Campos de informações de faturamento da AMI

Os campos a seguir fornecem informações de faturamento associadas a uma AMI:

Detalhes da plataforma

Os detalhes da plataforma associada ao código de faturamento da AMI. Por exemplo, Red Hat Enterprise Linux.

Operação de uso

A operação da instância do Amazon EC2 e o código de faturamento associado à AMI. Por exemplo, RunInstances:0010. A Usage operation (Operação de uso) corresponde à coluna [lineitem/Operation](#) (lineitem/Operação) no seu Relatório de custos e uso (CUR) da AWS e na [API de tabela de preços da AWS](#).

É possível visualizar esses campos na página Instances (Instâncias) ou AMIs no console do Amazon EC2 ou na resposta retornada pelo comando [describe-images](#).

Dados de amostra: operação de uso por plataforma

A tabela a seguir lista os detalhes da plataforma e os valores de operação de uso que podem ser exibidos na página Instances (Instâncias) ou AMIs no console do Amazon EC2 ou na resposta retornada pelo comando [describe-images](#).

Detalhes da plataforma	Operação de uso **
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux com HA	RunInstances:1010
Red Hat Enterprise Linux com SQL Server Standard e HA	RunInstances:1014
Red Hat Enterprise Linux com SQL Server Enterprise e HA	RunInstances:1110
Red Hat Enterprise Linux com SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux com SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux com SQL Server Enterprise	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200

Detalhes da plataforma	Operação de uso **
SUSE Linux	RunInstances:000g
Windows	RunInstances:0002
BYOL do Windows	RunInstances:0800
Windows com SQL Server Enterprise *	RunInstances:0102
Windows com SQL Server Standard *	RunInstances:0006
Windows com SQL Server Web *	RunInstances:0202

* Se duas licenças de software estiverem associadas a uma AMI, o campo Platform details (Detalhes da plataforma) mostrará as duas.

** Se você estiver executando as instâncias spot, o [lineitem/Operation](#) no Relatório de custos e uso da AWS poderá ser diferente do valor de Usage operation (Operação de uso) listado aqui. Por exemplo, se [lineitem/Operation](#) exibir RunInstances : 0010 : SV006, isso significará que o Amazon EC2 estará executando o Red Hat Enterprise Linux por hora de instância Spot no Leste dos EUA (Virgínia) na Zona número 6 da VPC.

Localizando detalhes de faturamento e uso da AMI

No console do Amazon EC2, você pode exibir as informações de faturamento da AMI na página AMIs ou na página Instances (Instâncias). Você também pode encontrar informações de faturamento usando a AWS CLI ou o serviço de metadados da instância.

Os campos a seguir podem ajudá-lo a verificar as cobranças da AMI em sua fatura:

- Detalhes da plataforma
- Operação de uso
- ID de AMI

Localizar informações de faturamento da AMI (console)

Siga estas etapas para visualizar as informações de faturamento da AMI no console da Amazon EC2:

Procure informações de faturamento da AMI na página AMIs

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha AMIs, e selecione uma AMI.
3. Na guia Details (Detalhes), verifique os valores para Platform details (Detalhes da plataforma) e Usage operation (Operação de uso).

Procure informações de faturamento da AMI na página Instances

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias) e selecione uma instância.
3. Na guia Details (Detalhes) (ou na guia Description (Descrição) , se você estiver usando a versão anterior do console, verifique os valores para Platform details (Detalhes da plataforma) e Usage operation (Operação de uso).

Localizar informações de faturamento da AMI (AWS CLI)

Para localizar as informações de faturamento da AMI usando a AWS CLI, você precisa saber o ID da AMI. Se não souber o ID da AMI, você pode obtê-lo na instância usando o comando [describe-instances](#) (Descrever instâncias).

Para localizar o ID da AMI

Se você souber o ID da instância, poderá obter o ID da AMI para a instância usando o comando [describe-instances](#) (Descrever instâncias).

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

No resultado, o ID da AMI é especificado no campo `ImageId`.

```
... "Instances": [
{
    "AmiLaunchIndex": 0,
    "ImageId": "ami-0123456789EXAMPLE",
    "InstanceId": "i-123456789abcde123",
    ...
}]
```

Para localizar as informações de faturamento da AMI

Se souber o ID da AMI, você pode usar o comando [describe-images](#) (Descrever imagens) para obter detalhes de operação de uso e da plataforma da AMI.

```
$ aws ec2 describe-images --image-ids ami-0123456789EXAMPLE
```

A saída do exemplo a seguir mostra os campos `PlatformDetails` e `UsageOperation`. Neste exemplo, a plataforma `ami-0123456789EXAMPLE` é Red Hat Enterprise Linux e a operação de uso e o código de faturamento é `RunInstances:0010`.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "Hypervisor": "xen",
            "EnaSupport": true,
            "SriovNetSupport": "simple",
            "ImageId": "ami-0123456789EXAMPLE",
            "State": "available",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2",
            "RootDeviceType": "ebs",
        }
    ]
}
```

```
        "OwnerId": "123456789012",
        "PlatformDetails": "Red Hat Enterprise Linux",
        "UsageOperation": "RunInstances:0010",
        "RootDeviceName": "/dev/sda1",
        "CreationDate": "2019-05-10T13:17:12.000Z",
        "Public": true,
        "ImageType": "machine",
        "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
    }
]
```

Verificar cobranças da AMI em sua fatura

Para garantir que você não incorra em custos não planejados, verifique se as informações de faturamento de uma instância no Relatório de custos e uso (CUR) da AWS correspondem às informações de faturamento associadas à AMI que você usou para executar a instância.

Para confirmar as informações de faturamento, localize o ID da instância no CUR e verifique o valor correspondente na coluna [lineitem/Operation](#). O valor deve corresponder ao valor da Usage operation (Operação de uso) associada à AMI.

Por exemplo, a AMI ami-0123456789EXAMPLE tem as seguintes informações de faturamento:

- Detalhes da plataforma = Red Hat Enterprise Linux
- Operação de uso = RunInstances:0010

Se você executou uma instância usando essa AMI, poderá localizar o ID da instância no CUR e verificar o valor correspondente na coluna [lineitem/Operation](#). Neste exemplo, o valor deve ser RunInstances:0010.

Instâncias do Amazon EC2

Se você for novo no Amazon EC2, consulte os seguintes tópicos para começar:

- [O que é o Amazon EC2? \(p. 1\)](#)
- [Configuração para usar o Amazon EC2. \(p. 6\)](#)
- [Tutorial: Comece a usar instâncias Windows do Amazon EC2 \(p. 10\)](#)
- [Ciclo de vida da instância \(p. 412\)](#)

Para executar um ambiente de produção, você precisará responder às seguintes perguntas.

P: Qual tipo de instância melhor atende às minhas necessidades?

O Amazon EC2 fornece tipos de instância diferentes para permitir que você escolha a CPU, a memória, o armazenamento e a capacidade de rede que você precisa para executar suas aplicações. Para obter mais informações, consulte [Tipos de instância \(p. 149\)](#).

P: Qual opção de compra melhor atende às minhas necessidades?

O Amazon EC2 oferece suporte a Instâncias on-demand (o padrão), Instâncias spot e Instâncias reservadas. Para obter mais informações, consulte [Opções de compra de instância \(p. 253\)](#).

P: Posso gerenciar remotamente uma frota de instâncias do EC2 e máquinas no meu ambiente híbrido?

O AWS Systems Manager permite gerenciar, de forma remota e segura, a configuração de suas instâncias do Amazon EC2, bem como suas instâncias e máquinas virtuais (VMs) on-premises em ambientes híbridos, incluindo VMs de outros provedores de nuvem. Para obter mais informações, consulte o [Guia do usuário do AWS Systems Manager](#).

Instâncias do Windows do Amazon EC2

Veja a seguir uma introdução aos principais componentes do Amazon EC2 e como uma instância do Windows se compara à execução do Windows Server no local.

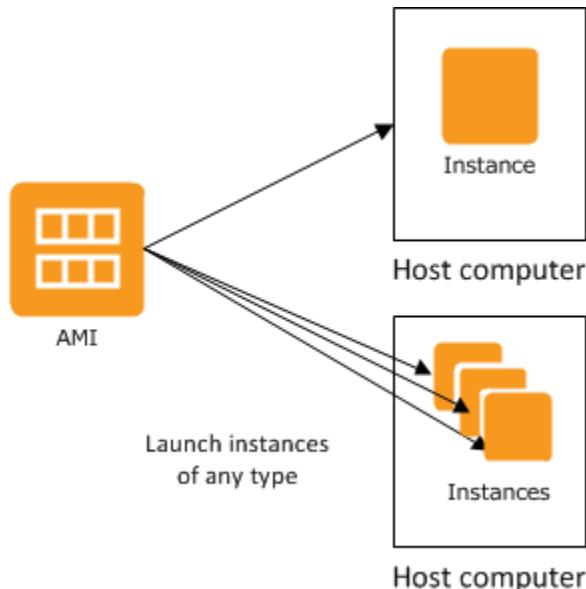
Instâncias e AMIs

Uma Imagem de máquina da Amazon (AMI) é um modelo que contém uma configuração de software (por exemplo, sistema operacional, servidor de aplicativo e aplicativos). Em uma AMI, você executa instâncias, que são cópias da AMI executadas como servidores virtuais na nuvem.

A Amazon publica muitas AMIs que contêm configurações de software comuns para uso público. Além disso, os membros da comunidade de desenvolvedores da AWS publicaram suas próprias AMIs personalizadas. Você também pode criar suas próprias AMIs personalizadas; isso permite iniciar com rapidez e facilidade as novas instâncias que têm tudo de que você precisa. Por exemplo, se sua aplicação for um site ou serviço Web, sua AMI poderá incluir um servidor Web, o conteúdo estático associado e o código para as páginas dinâmicas. Como resultado, depois de executar uma instância a partir dessa AMI, seu servidor web é iniciado e seu aplicativo fica pronto para aceitar solicitações.

Você pode executar diferentes tipos de instâncias a partir de uma única AMI. O tipo de instância determina essencialmente o hardware do computador host usado para sua instância. Cada tipo de instância

oferece recursos diferentes de computação e memória. Selecione um tipo de instância de acordo com a quantidade de capacidade de memória e computação necessária para as aplicações ou o software que você pretende executar na instância. Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte [Amazon EC2 Instance Types](#) (Tipos de instância do Amazon EC2). Você também pode executar várias instâncias de uma AMI, conforme mostrado na figura a seguir.



Suas instâncias do Windows continuarão sendo executadas até que você as interrompa ou encerre, ou até que elas falhem. Se uma instância falhar, você pode executar uma nova instância a partir da AMI.

Sua conta da AWS tem um limite quanto ao número de instâncias que você pode ter em execução. Para obter mais informações sobre esse limite e sobre como solicitar um aumento, consulte [Quantas instâncias posso executar no Amazon EC2](#) nas perguntas frequentes gerais do Amazon EC2.

Diferenças entre o Windows Server e instâncias do Windows

Depois que você executar uma instância do Windows do Amazon EC2, ela se comportará como um servidor tradicional que executa o Windows Server. Por exemplo, a instância do Windows Server e do Amazon EC2 pode ser usada para executar aplicações Web, conduzir processamentos em lotes ou gerenciar aplicações que exijam cálculos de grande escala. Contudo, há diferenças importantes entre o modelo de hardware de servidor e o modelo de computação em nuvem. A maneira como uma instância do Amazon EC2 é executada não é a mesma de um servidor tradicional executando o Windows Server.

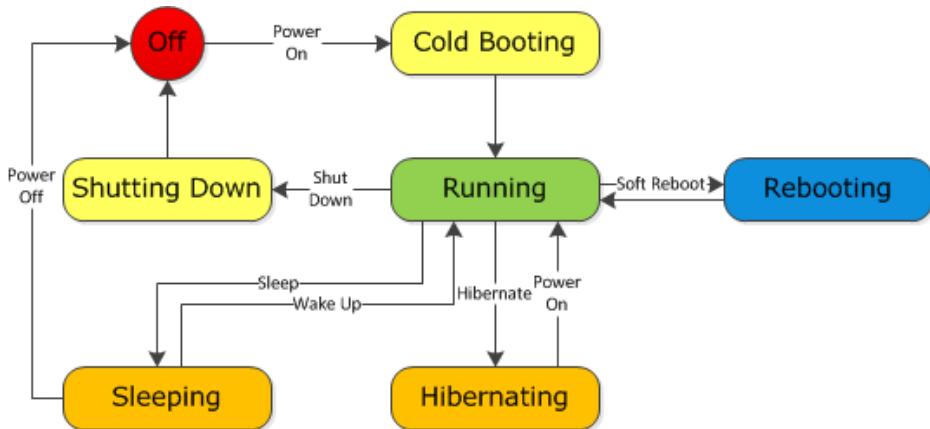
Antes de começar a executar instâncias do Windows do Amazon EC2, você deve estar ciente de que a arquitetura de aplicações em execução nos servidores de nuvem pode diferir significativamente em relação à arquitetura para modelos tradicionais de aplicações em execução no hardware. A implementação de aplicações nos servidores de nuvem requer uma mudança no processo de design.

A tabela a seguir descreve as principais diferenças entre instâncias do Windows Server e instâncias do Windows do Amazon EC2.

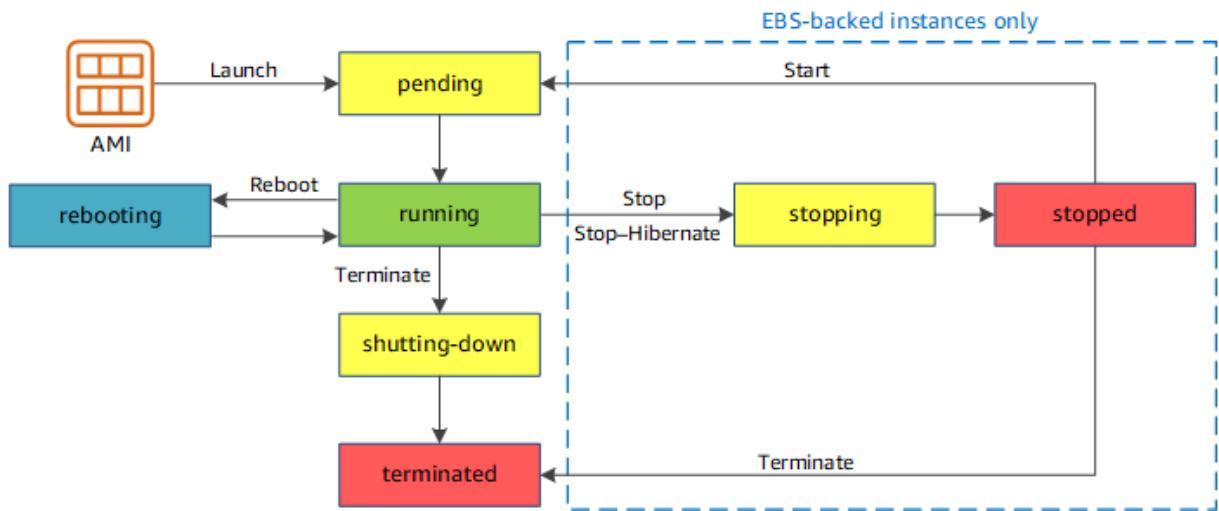
Windows Server	Instância do Windows do Amazon EC2
Recursos e capacidade são fisicamente limitados.	Recursos e capacidade são escaláveis.

Windows Server	Instância do Windows do Amazon EC2
Você paga pela infraestrutura, mesmo se não a usar.	Você paga pelo uso da infraestrutura. Paramos de cobrá-lo pela instância assim que você a interrompe ou encerra.
Ocupa espaço físico e deve ser mantida regularmente.	Não ocupa o espaço físico e não requer manutenção regular.
Inicia quando o botão de energia é pressionado (conhecido como inicialização a frio).	Inicia com a execução da instância.
Você pode manter o servidor em execução até a hora de desligá-lo ou colocá-lo no modo de suspensão ou hibernação (durante esse período, o servidor é desligado).	Você pode manter o servidor em execução ou interrompê-lo e reiniciá-lo (durante esse período, a instância é movida para um novo computador host).
Quando você desliga o servidor, todos os recursos permanecem intactos e no estado em que estavam quando ele foi desligado. As informações que você armazenou nos discos rígidos são mantidas e podem ser acessadas sempre que necessário. Você pode restaurar o servidor ao estado de execução ligando-o.	Quando você encerrar a instância, sua infraestrutura não estará mais disponível para você. Você não pode se conectar com uma instância ou reiniciá-la depois de tê-la encerrado. No entanto, pode criar uma imagem de sua instância durante a execução e executar novas instâncias da imagem a qualquer momento.

Um servidor tradicional que executa o Windows Server passa pelos estados mostrados no diagrama a seguir.



Uma instância do Windows do Amazon EC2 é semelhante ao Windows Server tradicional, como se pode ver comparando o diagrama a seguir com o diagrama anterior do Windows Server. Após a execução de uma instância, ela entra rapidamente no estado pendente enquanto o registro está sendo feito, depois entra no estado de execução. A instância permanece ativa até que você a interrompa ou encerre. Não é possível reiniciar uma instância depois de tê-la encerrado. Você pode criar uma imagem de backup de sua instância enquanto ela está em execução e executar uma nova instância da imagem de backup.



Projetar suas aplicações para serem executadas em instâncias do Windows

É importante considerar as diferenças mencionadas na seção anterior ao criar suas aplicações para execução nas instâncias do Windows do Amazon EC2.

Aplicações criadas para o Amazon EC2 usam a infraestrutura de computação subjacente conforme a necessidade. Eles utilizam recursos necessários (como armazenamento e computação) sob demanda para realizar um trabalho e abandonam os recursos quando terminam. Além disso, eles geralmente se desfazem de si próprios após a conclusão do trabalho. Enquanto está em operação, a aplicação aumenta ou diminui a escala de maneira elástica com base nos requisitos de recursos. Uma aplicação em execução em uma instância do Amazon EC2 pode encerrar e recriar os vários componentes à vontade em caso de falhas de infraestrutura.

Ao projetar as aplicações do Windows para execução no Amazon EC2, você pode planejar a rápida implantação e redução de recursos de computação e armazenamento, com base em suas necessidades em constante mudança.

Quando você executa uma instância de Windows do Amazon EC2, não precisa provisionar o pacote de sistema exato de hardware, software e armazenamento como faz com o Windows Server. Em vez disso, você pode se concentrar no uso de diversos recursos de nuvem para melhorar a escalabilidade e a performance global de sua aplicação do Windows.

Com o Amazon EC2, projetar para se proteger contra falhas e interrupções é uma parte integral e crucial da arquitetura. Assim como ocorre com qualquer sistema escalável e redundante, a arquitetura de seu sistema deve ser responsável pelas falhas de computação, redes e armazenamento. Você tem de criar mecanismos em suas aplicações que possam lidar com diferentes tipos de falhas. O segredo é criar um sistema modular com componentes individuais que não sejam intimamente ligados, possam interagir assincronamente e tratar um ao outro como caixas pretas que são independentemente escaláveis. Assim, se um dos componentes falhar ou estiver ocupado, você poderá executar mais instâncias desse componente sem corromper o sistema atual.

Outro elemento chave a ser projetado para proteger contra falhas é distribuir sua aplicação geograficamente. Replicar sua aplicação entre regiões geograficamente distribuídas aprimora a alta disponibilidade no sistema.

A infraestrutura do Amazon EC2 é programável e você pode usar scripts para automatizar o processo de implantação, instalar e configurar o software e aplicações e inicializar os servidores virtuais.

Você deve implementar segurança em cada camada de sua arquitetura de aplicação em execução em uma instância do Windows do Amazon EC2. Se você estiver preocupado em armazenar dados confidenciais no ambiente do Amazon EC2, deverá criptografar os dados antes do upload.

Tipos de instância

Quando executa uma instância, o tipo de instância que você especifica determina o hardware do computador host usado para sua instância. Cada tipo de instância oferece recursos de computação, memória e armazenamento diferentes, além de ser agrupado em famílias de instâncias de acordo com esses recursos. Selecione um tipo de instância com base nos requisitos da aplicação ou do software que você pretende executar na instância.

O Amazon EC2 fornece a cada instância uma quantidade consistente e previsível de capacidade de CPU, independentemente do hardware subjacente.

O Amazon EC2 dedica alguns recursos do computador host, como CPU, memória e armazenamento de instâncias, a uma instância específica. O Amazon EC2 compartilha outros recursos do computador host, como a rede e o subsistema de disco, entre instâncias. Se cada instância em um computador host tentar usar o máximo desses recursos compartilhados quanto for possível, cada uma receberá uma parte igual daquele recurso. No entanto, quando um recurso for pouco utilizado, uma instância poderá consumir uma parte maior desse recurso enquanto ele estiver disponível.

Cada tipo de instância fornece uma performance mínima superior ou inferior com base em um recurso compartilhado. Por exemplo, tipos de instância com performance alta de E/S têm uma alocação maior dos recursos compartilhados. A alocação de uma parte maior dos recursos compartilhados também reduz a variação da performance de E/S. Para a maioria das aplicações, a performance moderada de E/S é mais do que suficiente. No entanto, para aplicações que exigem uma performance de E/S maior ou mais consistente, considere um tipo de instância com performance mais alta de E/S.

Tópicos

- [Tipos de instâncias disponíveis \(p. 149\)](#)
- [Especificações de hardware \(p. 153\)](#)
- [Instâncias criadas no Sistema Nitro \(p. 154\)](#)
- [Recursos de redes e armazenamento \(p. 155\)](#)
- [Limites de instâncias \(p. 158\)](#)
- [Instâncias de uso geral \(p. 158\)](#)
- [Instâncias otimizadas para computação \(p. 204\)](#)
- [Instâncias otimizadas para memória \(p. 211\)](#)
- [Instâncias otimizadas para armazenamento \(p. 222\)](#)
- [Windows Instâncias computacionais aceleradas \(p. 228\)](#)
- [Localizar um tipo de instância do Amazon EC2 \(p. 242\)](#)
- [Alterar o tipo de instância \(p. 244\)](#)
- [Obter recomendações de um tipo de instância \(p. 249\)](#)

Tipos de instâncias disponíveis

O Amazon EC2 fornece uma ampla seleção de tipos de instância otimizadas para diferentes casos de uso. Para determinar quais tipos de instância atendem aos seus requisitos, como regiões compatíveis, recursos de computação ou recursos de armazenamento, consulte [Localizar um tipo de instância do Amazon EC2 \(p. 242\)](#).

Instâncias da geração atual

Para melhor performance, recomendamos que você use os seguintes tipos de instância quando executar novas instâncias. Para obter mais informações, consulte [Tipos de instância do Amazon EC2](#).

Tipo	Sizes	Caso de uso
C4	c4.large c4.xlarge c4.2xlarge c4.4xlarge c4.8xlarge	Otimizadas para computação (p. 204)
C5	c5.large c5.xlarge c5.2xlarge c5.4xlarge c5.9xlarge c5.12xlarge c5.18xlarge c5.24xlarge c5.metal	Otimizadas para computação (p. 204)
C5a	c5a.large c5a.xlarge c5a.2xlarge c5a.4xlarge c5a.8xlarge c5a.12xlarge c5a.16xlarge c5a.24xlarge	Otimizadas para computação (p. 204)
C5ad	c5ad.large c5ad.xlarge c5ad.2xlarge c5ad.4xlarge c5ad.8xlarge c5ad.12xlarge c5ad.16xlarge c5ad.24xlarge	Otimizadas para computação (p. 204)
C5d	c5d.large c5d.xlarge c5d.2xlarge c5d.4xlarge c5d.9xlarge c5d.12xlarge c5d.18xlarge c5d.24xlarge c5d.metal	Otimizadas para computação (p. 204)
C5n	c5n.large c5n.xlarge c5n.2xlarge c5n.4xlarge c5n.9xlarge c5n.18xlarge c5n.metal	Otimizadas para computação (p. 204)
D2	d2.xlarge d2.2xlarge d2.4xlarge d2.8xlarge	Otimizada para armazenamento (p. 222)
D3	d3.xlarge d3.2xlarge d3.4xlarge d3.8xlarge	Otimizada para armazenamento (p. 222)
D3en	d3en.large d3en.xlarge d3en.2xlarge d3en.4xlarge d3en.6xlarge d3en.8xlarge d3en.12xlarge	Otimizada para armazenamento (p. 222)
F1	f1.2xlarge f1.4xlarge f1.16xlarge	Computação acelerada (p. 228)
G3	g3s.xlarge g3.4xlarge g3.8xlarge g3.16xlarge	Computação acelerada (p. 228)
G4ad	g4ad.xlarge g4ad.2xlarge g4ad.4xlarge g4ad.8xlarge g4ad.16xlarge	Computação acelerada (p. 228)
G4dn	g4dn.xlarge g4dn.2xlarge g4dn.4xlarge g4dn.8xlarge g4dn.12xlarge g4dn.16xlarge g4dn.metal	Computação acelerada (p. 228)
H1	h1.2xlarge h1.4xlarge h1.8xlarge h1.16xlarge	Otimizada para armazenamento (p. 222)

Tipo	Sizes	Caso de uso
I3	i3.large i3.xlarge i3.2xlarge i3.4xlarge i3.8xlarge i3.16xlarge i3.metal	Otimizada para armazenamento (p. 222)
I3en	i3en.large i3en.xlarge i3en.2xlarge i3en.3xlarge i3en.6xlarge i3en.12xlarge i3en.24xlarge i3en.metal	Otimizada para armazenamento (p. 222)
M4	m4.large m4.xlarge m4.2xlarge m4.4xlarge m4.10xlarge m4.16xlarge	Propósito geral (p. 158)
M5	m5.large m5.xlarge m5.2xlarge m5.4xlarge m5.8xlarge m5.12xlarge m5.16xlarge m5.24xlarge m5.metal	Propósito geral (p. 158)
M5a	m5a.large m5a.xlarge m5a.2xlarge m5a.4xlarge m5a.8xlarge m5a.12xlarge m5a.16xlarge m5a.24xlarge	Propósito geral (p. 158)
M5ad	m5ad.large m5ad.xlarge m5ad.2xlarge m5ad.4xlarge m5ad.8xlarge m5ad.12xlarge m5ad.16xlarge m5ad.24xlarge	Propósito geral (p. 158)
M5d	m5d.large m5d.xlarge m5d.2xlarge m5d.4xlarge m5d.8xlarge m5d.12xlarge m5d.16xlarge m5d.24xlarge m5d.metal	Propósito geral (p. 158)
M5dn	m5dn.large m5dn.xlarge m5dn.2xlarge m5dn.4xlarge m5dn.8xlarge m5dn.12xlarge m5dn.16xlarge m5dn.24xlarge m5dn.metal	Propósito geral (p. 158)
M5n	m5n.large m5n.xlarge m5n.2xlarge m5n.4xlarge m5n.8xlarge m5n.12xlarge m5n.16xlarge m5n.24xlarge m5n.metal	Propósito geral (p. 158)
M5zn	m5zn.large m5zn.xlarge m5zn.2xlarge m5zn.3xlarge m5zn.6xlarge m5zn.12xlarge m5zn.metal	Propósito geral (p. 158)
M6i	m6i.large m6i.xlarge m6i.2xlarge m6i.4xlarge m6i.8xlarge m6i.12xlarge m6i.16xlarge m6i.24xlarge m6i.32xlarge	Propósito geral (p. 158)
P2	p2.xlarge p2.8xlarge p2.16xlarge	Computação acelerada (p. 228)
P3	p3.2xlarge p3.8xlarge p3.16xlarge	Computação acelerada (p. 228)
P3dn	p3dn.24xlarge	Computação acelerada (p. 228)
R4	r4.large r4.xlarge r4.2xlarge r4.4xlarge r4.8xlarge r4.16xlarge	Otimizado para memória (p. 211)
R5	r5.large r5.xlarge r5.2xlarge r5.4xlarge r5.8xlarge r5.12xlarge r5.16xlarge r5.24xlarge r5.metal	Otimizado para memória (p. 211)
R5a	r5a.large r5a.xlarge r5a.2xlarge r5a.4xlarge r5a.8xlarge r5a.12xlarge r5a.16xlarge r5a.24xlarge	Otimizado para memória (p. 211)

Tipo	Sizes	Caso de uso
R5ad	r5ad.large r5ad.xlarge r5ad.2xlarge r5ad.4xlarge r5ad.8xlarge r5ad.12xlarge r5ad.16xlarge r5ad.24xlarge	Otimizado para memória (p. 211)
R5b	r5b.large r5b.xlarge r5b.2xlarge r5b.4xlarge r5b.8xlarge r5b.12xlarge r5b.16xlarge r5b.24xlarge r5b.metal	Otimizado para memória (p. 211)
R5d	r5d.large r5d.xlarge r5d.2xlarge r5d.4xlarge r5d.8xlarge r5d.12xlarge r5d.16xlarge r5d.24xlarge r5d.metal	Otimizado para memória (p. 211)
R5dn	r5dn.large r5dn.xlarge r5dn.2xlarge r5dn.4xlarge r5dn.8xlarge r5dn.12xlarge r5dn.16xlarge r5dn.24xlarge r5dn.metal	Otimizado para memória (p. 211)
R5n	r5n.large r5n.xlarge r5n.2xlarge r5n.4xlarge r5n.8xlarge r5n.12xlarge r5n.16xlarge r5n.24xlarge r5n.metal	Otimizado para memória (p. 211)
T2	t2.nano t2.micro t2.small t2.medium t2.large t2.xlarge t2.2xlarge	Propósito geral (p. 158)
T3	t3.nano t3.micro t3.small t3.medium t3.large t3.xlarge t3.2xlarge	Propósito geral (p. 158)
T3a	t3a.nano t3a.micro t3a.small t3a.medium t3a.large t3a.xlarge t3a.2xlarge	Propósito geral (p. 158)
Alta memória (u-*)	u-6tb1.56xlarge u-6tb1.112xlarge u-6tb1.metal u-9tb1.112xlarge u-9tb1.metal u-12tb1.112xlarge u-12tb1.metal u-18tb1.metal u-24tb1.metal	Otimizado para memória (p. 211)
X1	x1.16xlarge x1.32xlarge	Otimizado para memória (p. 211)
X1e	x1e.xlarge x1e.2xlarge x1e.4xlarge x1e.8xlarge x1e.16xlarge x1e.32xlarge	Otimizado para memória (p. 211)
z1d	z1d.large z1d.xlarge z1d.2xlarge z1d.3xlarge z1d.6xlarge z1d.12xlarge z1d.metal	Otimizado para memória (p. 211)

Instâncias da geração anterior

A Amazon Web Services oferece tipos de instâncias da geração anterior para usuários que otimizaram suas aplicações com base nelas e ainda precisam atualizá-los. Recomendamos que você use os tipos de instância da geração atual para obter a melhor performance, mas continuamos a oferecer suporte aos seguintes tipos de instância da geração anterior. Para obter mais informações sobre qual tipo de instância da geração atual seria uma atualização adequada, consulte [Instâncias da geração anterior](#).

Tipo	Sizes
C1	c1.medium c1.xlarge
C3	c3.large c3.xlarge c3.2xlarge c3.4xlarge c3.8xlarge
G2	g2.2xlarge g2.8xlarge
I2	i2.xlarge i2.2xlarge i2.4xlarge i2.8xlarge
M1	m1.small m1.medium m1.large m1.xlarge
M2	m2.xlarge m2.2xlarge m2.4xlarge
M3	m3.medium m3.large m3.xlarge m3.2xlarge
R3	r3.large r3.xlarge r3.2xlarge r3.4xlarge r3.8xlarge
T1	t1.micro

Especificações de hardware

Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte [Amazon EC2 Instance Types](#) (Tipos de instância do Amazon EC2).

Para determinar que tipo de instância atende melhor às suas necessidades, recomendamos executar uma instância e usar seu própria aplicação de referência. Como você paga pelo segundo da instância, é conveniente e econômico testar vários tipos de instância antes de tomar uma decisão.

Se suas necessidades mudarem, mesmo após ter tomado uma decisão, você poderá redimensionar a instância posteriormente. Para obter mais informações, consulte [Alterar o tipo de instância \(p. 244\)](#).

Note

Normalmente, as instâncias do Amazon EC2 são executadas em processadores virtuais Intel de 64 bits, como especificado nas páginas de produto do tipo de instância. Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte [Amazon EC2 Instance Types](#) (Tipos de instância do Amazon EC2). Contudo, pode haver confusão com as convenções de nomenclatura do setor para CPUs de 64 bits. A fabricante de chips Advanced Micro Devices (AMD) apresentou a primeira arquitetura 64 bits comercialmente bem-sucedida com base no conjunto de instruções do Intel x86. Consequentemente, a arquitetura é amplamente referida como AMD64, independente do fabricante do chip. O Windows e várias distribuições do Linux adotam essa prática. Isso explica por que as informações internas do sistema em uma instância do EC2 Ubuntu ou Windows exibe a arquitetura de CPU como AMD64, ainda que as instâncias estejam sendo executadas em hardware Intel.

Processor features (Recursos do processador)

Recursos do processador Intel

Amazon EC2 as instâncias executadas nos processadores Intel podem incluir os seguintes recursos. Nem todos os recursos de processador a seguir são compatíveis com todos os tipos de instância. Para obter informações detalhadas sobre quais recursos estão disponíveis para cada tipo de instância, consulte [Tipos de instância do Amazon EC2](#).

- Intel AES New Instructions (AES-NI) — O conjunto de instruções de criptografia Intel AES-NI aprimora o algoritmo Advanced Encryption Standard (AES) original para oferecer proteção de dados mais rápida

e maior segurança. Todas as instâncias do EC2 da geração atual oferecem suporte a esse recurso de processador.

- Intel Advanced Vector Extensions (Intel AVX, Intel AVX2 e AVX-512): o Intel AVX e o Intel AVX2 são extensões de conjunto de instruções de 256 bits e o Intel AVX-512 é uma extensão de conjunto de instruções de 512 bits projetadas para aplicações com uso intensivo de Floating Point (FP – Ponto flutuante). As instruções Intel AVX melhoram a performance de aplicações, como de processamento de imagem, áudio e vídeo, simulações científicas, análise financeira e modelagem e análise 3D. Esses recursos só estão disponíveis em instâncias executadas com AMIs de HVM.
- Tecnologia Intel Turbo Boost — Os processadores com Tecnologia Intel Turbo Boost executam núcleos automaticamente com mais rapidez do que a frequência operacional básica.
- Intel Deep Learning Boost (Intel DL Boost) — Acelera os casos de uso de deep learning profundo da IA. Os processadores Intel Xeon Scalable da segunda geração ampliam o Intel AVX-512 com uma nova Vector Neural Network Instruction (VNNI/INT8), que aumenta significativamente a performance de inferência de deep learning em comparação com a geração anterior dos processadores Intel Xeon Scalable (com FP32), para reconhecimento/segmentação de imagens, detecção de objetos, reconhecimento de fala, tradução de idiomas, sistemas de recomendação, aprendizado por reforço e outros. A VNNI pode não ser compatível com todas as distribuições Linux.

As seguintes instâncias oferecem suporte a VNNI: M5nR5nM5dnM5znR5b, R5dn, D3 e D3en. As instâncias C5 e C5d só oferecem à VNNI para as instâncias 12xlarge, 24xlarge e metal.

Instâncias criadas no Sistema Nitro

O Sistema Nitro é uma coleção de hardware e componentes de software criados pela AWS que permitem alta performance, alta disponibilidade e alta segurança. Para obter mais informações, consulte [AWS Nitro System](#).

O Sistema Nitro fornece recursos bare metal que eliminam a sobrecarga da virtualização e oferecem suporte a workloads que exigem acesso total ao hardware do host. Instâncias bare metal são ideais para o seguinte:

- Workloads que exigem acesso a recursos de hardware de baixo nível (por exemplo, Intel VT) que não estão disponíveis ou não são totalmente compatíveis ambientes virtualizados
- Aplicações que exigem um ambiente não virtualizado para licenciamento ou suporte

Componentes do Nitro

Os componentes a seguir fazem parte do Sistema Nitro:

- Nitro Card
 - Volumes de armazenamento NVMe locais
 - Suporte a hardware de rede
 - Gerenciamento
 - Monitoramento
 - Segurança
- Nitro Security Chip, integrado na placa-mãe
- Hipervisor do Nitro: um hipervisor leve que gerencia a alocação de memória e de CPU e fornece performance que não é diferenciada de bare metal para a maioria das workloads.

Tipos de instância

As instâncias a seguir são criadas no sistema Nitro:

- Virtualizadas: C5, C5a, C5ad, C5d, C5n, D3, D3en, G4, I3en, M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6i, p3dn.24xlarge, R5, R5a, R5ad, R5b, R5d, R5dn, R5n, T3, T3a, alta memória (u-*), e z1d
- Bare metal: c5.metal, c5d.metal, c5n.metal, i3.metal, i3en.metal, m5.metal, m5d.metal, m5dn.metal, m5n.metal, m5zn.metal, r5.metal, r5b.metal, r5d.metal, r5dn.metal, r5n.metal, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal, e z1d.metal

Saiba mais

Para obter mais informações, assista aos seguinte vídeos:

- AWS re:Invent 2017: The Amazon EC2 Nitro System Architecture
- AWS re:Invent 2017: Amazon EC2 Bare Metal Instances
- AWS re:Invent 2019: Powering next-gen Amazon EC2: Deep dive into the Nitro system
- AWS re:Inforce 2019: Security Benefits of the Nitro Architecture

Recursos de redes e armazenamento

Ao selecionar um tipo de instância, isso determinará os recursos de rede e armazenamento disponíveis. Para descrever um tipo de instância, use o comando [describe-instance-types](#).

Recursos de redes

- O IPv6 é compatível com todos os tipos de instância da geração atual e com os tipos de instância C3, R3 e I2 das gerações anteriores.
- Para maximizar a performance de rede e largura de banda do seu tipo de instância, você pode fazer o seguinte:
 - Execute os tipos de instância compatíveis em um placement group de cluster para otimizar as instâncias de aplicações de computação de alta performance (HPC). As instâncias em um placement group de cluster comum podem se beneficiar de redes de alta largura de banda e baixa latência. Para obter mais informações, consulte [Grupos de posicionamento \(p. 1044\)](#).
 - Habilite rede avançada para tipos de instâncias da geração atual compatíveis para obter performance significativamente maior de pacotes por segundo (PPS), jitter de rede mais baixo e latências mais baixas. Para obter mais informações, consulte [Rede avançada no Windows \(p. 1028\)](#).
- Os tipos de instância da geração atual habilitados para redes aprimoradas têm os seguintes atributos de performance de rede:
 - O tráfego dentro da mesma região com endereços IPv4 ou IPv6 privados pode dar suporte a 5 Gbps para o tráfego de fluxo único e a até 25 Gbps para o tráfego de vários fluxos (dependendo do tipo da instância).
 - O tráfego para e de buckets do Amazon S3 dentro da mesma região pelo espaço de endereço IP público ou por um VPC endpoint pode usar toda a largura de banda agregada da instância disponível.
 - A unidade de transmissão máxima (MTU) compatível varia de acordo com os tipos de instância. Todos os tipos de instância do Amazon EC2 oferecem suporte a frames Ethernet V2 de 1500 MTU. Todas as instâncias da geração atual são compatíveis com 9001 MTU, ou frames jumbo, de forma que as instâncias da geração anterior também oferecem suporte a elas. Para obter mais informações, consulte [Unidade de transmissão máxima \(MTU\) de rede para a instância do EC2 \(p. 1056\)](#).

Características do armazenamento

- Alguns tipos de instância oferecem suporte a volumes do EBS e volumes de armazenamento de instâncias, enquanto outros tipos de instância suportam só volumes do EBS. Alguns tipos de instância

que oferecem suporte a volumes de armazenamento de instâncias usam solid state drives (SSD) para oferecer performance de E/S aleatória muita alta. Alguns tipos de instância oferecem suporte a volumes de armazenamento de instâncias NVMe. Alguns tipos de instância oferecem suporte a volumes de EBS NVMe. Para obter mais informações, consulte [Amazon EBS e NVMe em instâncias Windows \(p. 1438\)](#) e [Volumes SSD de NVMe \(p. 1503\)](#).

- Para obter capacidade adicional e dedicada para E/S do Amazon EBS, você pode executar alguns tipos de instância na forma de instâncias otimizadas para EBS. Alguns tipos de instância são otimizadas para EBS por padrão. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

Resumo de recursos de redes e armazenamento

A tabela a seguir resume os recursos de rede e armazenamento compatíveis com os tipos de instância da geração atual.

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group	Redes avançadas
C4	Sim	Não	Não	Sim	Intel 82599 VF
C5	Sim	Sim	Não	Sim	ENA
C5a	Sim	Sim	Não	Sim	ENA
C5ad	Não	Sim	NVMe *	Sim	ENA
C5d	Não	Sim	NVMe *	Sim	ENA
C5n	Sim	Sim	Não	Sim	ENA
D2	Não	Não	HDD	Sim	Intel 82599 VF
D3	Não	Sim	NVMe *	Sim	ENA
D3en	Não	Sim	NVMe *	Sim	ENA
F1	Não	Não	NVMe *	Sim	ENA
G3	Sim	Não	Não	Sim	ENA
G4ad	Não	Sim	NVMe *	Sim	ENA
G4dn	Não	Sim	NVMe *	Sim	ENA
H1	Não	Não	HDD*	Sim	ENA
I3	Não	Não	NVMe *	Sim	ENA
I3en	Não	Sim	NVMe *	Sim	ENA
M4	Sim	Não	Não	Sim	m4.16xlarge: ENA Todos os outros tamanhos: Intel 82599 VF
M5	Sim	Sim	Não	Sim	ENA

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group	Redes avançadas
M5a	Sim	Sim	Não	Sim	ENA
M5ad	Não	Sim	NVMe *	Sim	ENA
M5d	Não	Sim	NVMe *	Sim	ENA
M5dn	Não	Sim	NVMe *	Sim	ENA
M5n	Sim	Sim	Não	Sim	ENA
M5zn	Sim	Sim	Não	Sim	ENA
M6i	Sim	Sim	Não	Sim	ENA
P2	Sim	Não	Não	Sim	ENA
P3	Sim	Não	Não	Sim	ENA
P3dn	Não	Sim	NVMe *	Sim	ENA
R4	Sim	Não	Não	Sim	ENA
R5	Sim	Sim	Não	Sim	ENA
R5a	Sim	Sim	Não	Sim	ENA
R5ad	Não	Sim	NVMe *	Sim	ENA
R5b	Sim	Sim	Não	Sim	ENA
R5d	Não	Sim	NVMe *	Sim	ENA
R5dn	Não	Sim	NVMe *	Sim	ENA
R5n	Sim	Sim	Não	Sim	ENA
T2	Sim	Não	Não	Não	Não
T3	Sim	Sim	Não	Não	ENA
T3a	Sim	Sim	Não	Não	ENA
Alta memória (u-*)	Sim	Sim	Não	Virtualizada: sim Bare metal: não	ENA
X1	Não	Não	SSD*	Sim	ENA
X1e	Não	Não	SSD*	Sim	ENA
z1d	Não	Sim	NVMe *	Sim	ENA

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

A tabela a seguir resume os recursos de rede e armazenamento compatíveis com os tipos de instância da geração anterior.

	Armazenamento de instâncias	Placement group	Redes avançadas
C3	SSD	Sim	Intel 82599 VF
G2	SSD	Sim	Não
I2	SSD	Sim	Intel 82599 VF
M3	SSD	Não	Não
R3	SSD	Sim	Intel 82599 VF

Limites de instâncias

Existe um limite sobre o número total de instâncias que você pode executar em uma região, e limites adicionais sobre alguns tipos de instância.

Para obter mais informações sobre os limites padrão, consulte [Quantas instâncias posso executar no Amazon EC2?](#)

Para obter mais informações sobre como visualizar os limites atuais ou solicitar aumento dos limites atuais, consulte [Cotas de serviço do Amazon EC2 \(p. 1567\)](#).

Instâncias de uso geral

As instâncias de uso geral oferecem um equilíbrio entre recursos de computação, memória e redes, e podem ser usadas em uma grande variedade de workloads.

Instâncias M5 e M5a

Essas instâncias fornecem uma infraestrutura em nuvem ideal, oferecendo um equilíbrio entre recursos de computação, memória e redes para uma ampla variedade de aplicações implantadas na nuvem. Elas são ideais para o seguinte:

- Bancos de dados de pequeno e médio portes
- Tarefas de processamento de dados que requerem memória adicional
- Frotas de cache
- Servidores de backend para SAP, Microsoft SharePoint, computação em cluster e outras aplicações corporativas

Para obter mais informações, consulte [Instâncias M5 do Amazon EC2](#).

As instâncias bare metal, como a m5.meta1, fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória.

M5zn

Essas instâncias são ideais para aplicações que se beneficiam de uma performance extremamente alta de thread único, alta taxa de transferência e rede de baixa latência. Elas são ideais para o seguinte:

- Jogos
- Computação de alta performance
- Modelagem de simulação

Para obter mais informações, consulte [Instâncias M5 do Amazon EC2](#).

As instâncias bare metal, como a `m5zn.metal`, fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória.

Instâncias M6i

Essas instâncias são ideais para workloads de uso geral, como as seguintes:

- Servidores de aplicações e servidores Web
- Microsserviços
- Computação de alta performance
- Desenvolvimento de aplicações
- Bancos de dados de pequeno e médio portes
- Frotas de cache

Para obter mais informações, consulte [Instâncias M6i do Amazon EC2](#).

Instâncias T2, T3 e T3a

Essas instâncias fornecem um nível de linha de base de performance de CPU com a capacidade de intermitência até um nível superior quando exigido por sua workload. Uma instância ilimitada pode sustentar alta performance de CPU por qualquer período, sempre que necessário. Para obter mais informações, consulte [Instâncias expansíveis \(p. 169\)](#). Elas são ideais para o seguinte:

- Sites e aplicações Web
- Repositórios de códigos
- Ambientes de desenvolvimento, criação, teste e preparação
- Microsserviços

Para obter mais informações, consulte [Instâncias T2 do Amazon EC2](#) e [Instâncias T3 do Amazon EC2](#).

Tópicos

- [Especificações de hardware \(p. 159\)](#)
- [Da performance da instância \(p. 163\)](#)
- [Performance das redes \(p. 163\)](#)
- [Performance de E/S em SSD \(p. 166\)](#)
- [Recursos da instância \(p. 167\)](#)
- [Notas de release \(p. 168\)](#)
- [Instâncias expansíveis \(p. 169\)](#)

Especificações de hardware

Este é um resumo das especificações de hardware para instâncias de uso geral.

Tipo de instância	vCPUs padrão	Memória (GiB)
<code>m4.large</code>	2	8
<code>m4.xlarge</code>	4	16
<code>m4.2xlarge</code>	8	32

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Propósito geral

Tipo de instância	vCPUs padrão	Memória (GiB)
m4.4xlarge	16	64
m4.10xlarge	40	160
m4.16xlarge	64	256
m5.large	2	8
m5.xlarge	4	16
m5.2xlarge	8	32
m5.4xlarge	16	64
m5.8xlarge	32	128
m5.12xlarge	48	192
m5.16xlarge	64	256
m5.24xlarge	96	384
m5.metal	96	384
m5a.large	2	8
m5a.xlarge	4	16
m5a.2xlarge	8	32
m5a.4xlarge	16	64
m5a.8xlarge	32	128
m5a.12xlarge	48	192
m5a.16xlarge	64	256
m5a.24xlarge	96	384
m5ad.large	2	8
m5ad.xlarge	4	16
m5ad.2xlarge	8	32
m5ad.4xlarge	16	64
m5ad.8xlarge	32	128
m5ad.12xlarge	48	192
m5ad.16xlarge	64	256
m5ad.24xlarge	96	384
m5d.large	2	8
m5d.xlarge	4	16
m5d.2xlarge	8	32

Tipo de instância	vCPUs padrão	Memória (GiB)
m5d.4xlarge	16	64
m5d.8xlarge	32	128
m5d.12xlarge	48	192
m5d.16xlarge	64	256
m5d.24xlarge	96	384
m5d.metal	96	384
m5dn.large	2	8
m5dn.xlarge	4	16
m5dn.2xlarge	8	32
m5dn.4xlarge	16	64
m5dn.8xlarge	32	128
m5dn.12xlarge	48	192
m5dn.16xlarge	64	256
m5dn.24xlarge	96	384
m5dn.metal	96	384
m5n.large	2	8
m5n.xlarge	4	16
m5n.2xlarge	8	32
m5n.4xlarge	16	64
m5n.8xlarge	32	128
m5n.12xlarge	48	192
m5n.16xlarge	64	256
m5n.24xlarge	96	384
m5n.metal	96	384
m5zn.large	2	8
m5zn.xlarge	4	16
m5zn.2xlarge	8	32
m5zn.3xlarge	12	48
m5zn.6xlarge	24	96
m5zn.12xlarge	48	192
m5zn.metal	48	192

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Propósito geral

Tipo de instância	vCPUs padrão	Memória (GiB)
m6i.large	2	8
m6i.xlarge	4	16
m6i.2xlarge	8	32
m6i.4xlarge	16	64
m6i.8xlarge	32	128
m6i.12xlarge	48	192
m6i.16xlarge	64	256
m6i.24xlarge	96	384
m6i.32xlarge	128	512
t2.nano	1	0,5
t2.micro	1	1
t2.small	1	2
t2.medium	2	4
t2.large	2	8
t2.xlarge	4	16
t2.2xlarge	8	32
t3.nano	2	0,5
t3.micro	2	1
t3.small	2	2
t3.medium	2	4
t3.large	2	8
t3.xlarge	4	16
t3.2xlarge	8	32
t3a.nano	2	0,5
t3a.micro	2	1
t3a.small	2	2
t3a.medium	2	4
t3a.large	2	8
t3a.xlarge	4	16
t3a.2xlarge	8	32

Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte [Amazon EC2 Instance Types](#) (Tipos de instância do Amazon EC2).

Para obter mais informações sobre como especificar opções de CPU, consulte [Otimizar as opções de CPU](#) (p. 582).

Da performance da instância

As instâncias otimizadas para EBS permitem que você tenha uma performance consistentemente alta para seus volumes do EBS ao eliminar a contenção entre E/S do Amazon EBS e outros tráfegos de rede da sua instância. Algumas instâncias de uso geral são otimizadas para EBS por padrão, sem nenhum custo adicional. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS](#) (p. 1440).

Performance das redes

É possível habilitar a rede avançada em tipos de instâncias compatíveis para fornecer latências mais baixas, jitter de rede mais baixo e melhor performance de pacotes por segundo (PPS). A maioria das aplicações não precisa de um alto nível de performance de rede constantemente, mas pode se beneficiar com uma largura de banda maior ao enviar ou receber dados. Para obter mais informações, consulte [Rede avançada no Windows](#) (p. 1028).

Este é um resumo da performance de rede para instâncias de uso geral que oferecem suporte às redes aprimoradas.

Tipo de instância	Performance das redes	Redes avançadas
T2	Até 1 Gbps	Sem suporte
T3 T3a	Até 5 Gbps †	ENA (p. 1029)
m4.large	Moderada	Intel 82599 VF (p. 1037)
m4.xlarge m4.2xlarge m4.4xlarge	Alto	Intel 82599 VF (p. 1037)
m5.4xlarge e menor m5a.8xlarge e menor m5ad.8xlarge e menor m5d.4xlarge e menor	Até 10 Gbps †	ENA (p. 1029)
m4.10xlarge	10 Gbps	Intel 82599 VF (p. 1037)
m5.8xlarge m5.12xlarge m5a.12xlarge m5ad.12xlarge m5d.8xlarge m5d.12xlarge	10 Gbps	ENA (p. 1029)
m5a.16xlarge m5ad.16xlarge	12 Gbps	ENA (p. 1029)
m6i.4xlarge e menor	Até 12,5 Gbps †	ENA (p. 1029)
m6i.8xlarge	12,5 Gbps	ENA (p. 1029)
m6i.12xlarge	18,75 Gbps	ENA (p. 1029)
m5.16xlarge m5a.24xlarge m5ad.24xlarge m5d.16xlarge	20 Gbps	ENA (p. 1029)

Tipo de instância	Performance das redes	Redes avançadas
m5dn.4xlarge e menor m5n.4xlarge e menor m5zn.3xlarge e menor	Até 25 Gbps †	ENA (p. 1029)
m4.16xlarge m5.24xlarge m5.metal m5d.24xlarge m5d.metal m5dn.8xlarge m5n.8xlarge m6i.16xlarge	25 Gbps	ENA (p. 1029)
m6i.24xlarge	37,5 Gbps	ENA (p. 1029)
m5dn.12xlarge m5n.12xlarge m5zn.6xlarge m6i.32xlarge	50 Gbps	ENA (p. 1029)
m5dn.16xlarge m5n.16xlarge	75 Gbps	ENA (p. 1029)
m5dn.24xlarge m5dn.metal m5n.24xlarge m5n.metal m5zn.12xlarge m5zn.metal	100 Gbps	ENA (p. 1029)

† Estas instâncias têm uma largura de banda de linha de base e podem usar um mecanismo de crédito de E/S de rede para ultrapassar sua largura de banda de linha de base conforme o melhor esforço. Para obter mais informações, consulte a [largura de banda da rede \(p. 1026\)](#).

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
m5.large	.75	10
m5.xlarge	1.25	10
m5.2xlarge	2,5	10
m5.4xlarge	5	10
m5a.large	.75	10
m5a.xlarge	1.25	10
m5a.2xlarge	2,5	10
m5a.4xlarge	5	10
m5ad.large	.75	10
m5ad.xlarge	1.25	10
m5ad.2xlarge	2,5	10
m5ad.4xlarge	5	10
m5d.large	.75	10
m5d.xlarge	1.25	10

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
m5d.2xlarge	2,5	10
m5d.4xlarge	5	10
m5dn.large	2.1	25
m5dn.xlarge	4.1	25
m5dn.2xlarge	8.125	25
m5dn.4xlarge	16.25	25
m5n.large	2.1	25
m5n.xlarge	4.1	25
m5n.2xlarge	8.125	25
m5n.4xlarge	16.25	25
m5zn.large	3	25
m5zn.xlarge	5	25
m5zn.2xlarge	10	25
m5zn.3xlarge	15	25
m6i.large	.781	12,5
m6i.xlarge	1.562	12,5
m6i.2xlarge	3.125	12,5
m6i.4xlarge	6.25	12,5
t3.nano	.032	5
t3.micro	.064	5
t3.small	.128	5
t3.medium	.256	5
t3.large	.512	5
t3.xlarge	1.024	5
t3.2xlarge	2.048	5
t3a.nano	.032	5
t3a.micro	.064	5
t3a.small	.128	5
t3a.medium	.256	5
t3a.large	.512	5

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
t3a.xlarge	1.024	5
t3a.2xlarge	2.048	5

Performance de E/S em SSD

Se você utilizar todos os volumes de armazenamento de instâncias baseados em SSD disponíveis para sua instância, você obterá a performance de IOPS (tamanho de bloco de 4.096 bytes) na tabela a seguir (na saturação de profundidade de fila). Do contrário, você terá uma performance de IOPS inferior.

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
m5ad.large *	30.000	15.000
m5ad.xlarge *	59.000	29.000
m5ad.2xlarge *	117.000	57.000
m5ad.4xlarge *	234.000	114.000
m5ad.8xlarge	466.666	233.333
m5ad.12xlarge	700.000	340.000
m5ad.16xlarge	933.333	466.666
m5ad.24xlarge	1.400.000	680.000
m5d.large *	30.000	15.000
m5d.xlarge *	59.000	29.000
m5d.2xlarge *	117.000	57.000
m5d.4xlarge *	234.000	114.000
m5d.8xlarge	466.666	233.333
m5d.12xlarge	700.000	340.000
m5d.16xlarge	933.333	466.666
m5d.24xlarge	1.400.000	680.000
m5d.metal	1.400.000	680.000
m5dn.large *	30.000	15.000
m5dn.xlarge *	59.000	29.000
m5dn.2xlarge *	117.000	57.000
m5dn.4xlarge *	234.000	114.000
m5dn.8xlarge	466.666	233.333

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
m5dn.12xlarge	700,000	340,000
m5dn.16xlarge	933.333	466.666
m5dn.24xlarge	1,400,000	680,000
m5dn.metal	1,400,000	680,000

* Para essas instâncias, você pode obter a performance especificada.

Ao preencher os volumes baseados de armazenamento de instâncias baseados em SSD, o número de IOPS de gravação que você pode atingir diminui. Isso se deve ao trabalho extra que o controlador SSD deve fazer para encontrar espaço disponível, regravar os dados existentes e apagar o espaço não utilizado para que possa ser regravado. Esse processo de coleta de lixo resulta em uma amplificação da gravação interna no SSD, expressa como uma proporção entre as operações de gravação SSD e as operações de gravação do usuário. Essa redução na performance será ainda maior se as operações de gravação não ocorrerem em múltiplos de 4.096 bytes ou não estiverem alinhadas com um limite de 4.096 bytes. Se você gravar uma quantidade menor de bytes ou os bytes que não estejam alinhados, o controlador SSD deverá ler os dados adjacentes e armazenar o resultado em um novo local. Esse padrão resulta em uma amplificação da gravação muito maior, maior latência e uma performance de E/S drasticamente reduzida.

Os controladores SSD podem usar várias estratégias para reduzir o impacto da amplificação da gravação. Uma dessas estratégias é reservar espaço no armazenamento de instâncias SSD para que o controlador possa gerenciar, com mais eficiência, o espaço disponível para operações de gravação. Isso é denominado superprovisionamento. Os volumes de armazenamento de instâncias baseados em SSD fornecidos a uma instância não têm espaço reservado para o superprovisionamento. Para reduzir a amplificação da gravação, recomendamos que você deixe 10% do volume não particionado de modo que o controlador SSD possa usá-lo para superprovisionamento. Isso diminui o armazenamento que você pode usar, mas aumenta a performance mesmo se o disco estiver próximo da capacidade total.

Para volumes de armazenamento de instâncias que oferecem suporte a TRIM, você pode usar o comando TRIM para notificar o controlador de SSD sempre quando você não precisa mais dos dados que gravou. Isso fornece ao controlador mais espaço livre, o que pode reduzir a amplificação da gravação e aumentar a performance. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 1504\)](#).

Recursos da instância

Este é um resumo dos recursos de instâncias de uso geral:

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
M4	Sim	Não	Não	Sim
M5	Sim	Sim	Não	Sim
M5a	Sim	Sim	Não	Sim
M5ad	Não	Sim	NVMe *	Sim
M5d	Não	Sim	NVMe *	Sim
M5dn	Não	Sim	NVMe *	Sim

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
M5n	Sim	Sim	Não	Sim
M5zn	Sim	Sim	Não	Sim
M6i	Sim	Sim	Não	Sim
T2	Sim	Não	Não	Não
T3	Sim	Sim	Não	Não
T3a	Sim	Sim	Não	Não

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

Para obter mais informações, consulte:

- [Amazon EBS e NVMe em instâncias Windows \(p. 1438\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#)
- [Grupos de posicionamento \(p. 1044\)](#)

Notas de release

- As instâncias M5, M5d e T3 têm um processador da série Intel Xeon Platinum 8000 de 3,1 GHz da primeira geração (Skylake-SP) ou da segunda geração (Cascade Lake).
- As instâncias M5a, M5ad e T3a têm um processador da série AMD EPYC 7000 de 2,5 GHz.
- As instâncias M5zn são alimentadas por CPUs Intel Cascade Lake que oferecem frequência turbo de até 4,5 GHz e largura de banda de rede de até 100 Gbps.
- As instâncias M6i apresentam processadores Intel Xeon Scalable de terceira geração (Ice Lake) e são compatíveis com o conjunto de instruções Intel Advanced Vector Extensions 512 (Intel AVX-512).
- Instâncias criadas no [Sistema Nitro \(p. 154\)](#), dos tipos de instância M4, t2.large e maiores, t3.large e maiores e t3a.large e maiores, exigem AMIs HVM de 64 bits. Elas têm mais memória e exigem um sistema operacional de 64 bits para tirar proveito dessa capacidade. As AMIs HVM fornecem performance superior em comparação com uso de AMIs paravirtuais (PV) em tipos de instância com mais memória. Além disso, você deve usar a AMI HVM para aproveitar a rede maior.
- As instâncias criadas no [Sistema Nitro \(p. 154\)](#) têm os seguintes requisitos:
 - Os [drivers de NVMe \(p. 1438\)](#) devem estar instalados
 - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1029\)](#) devem estar instalados

As [AMIs do Windows da AWS \(p. 29\)](#) atuais atendem a esses requisitos.

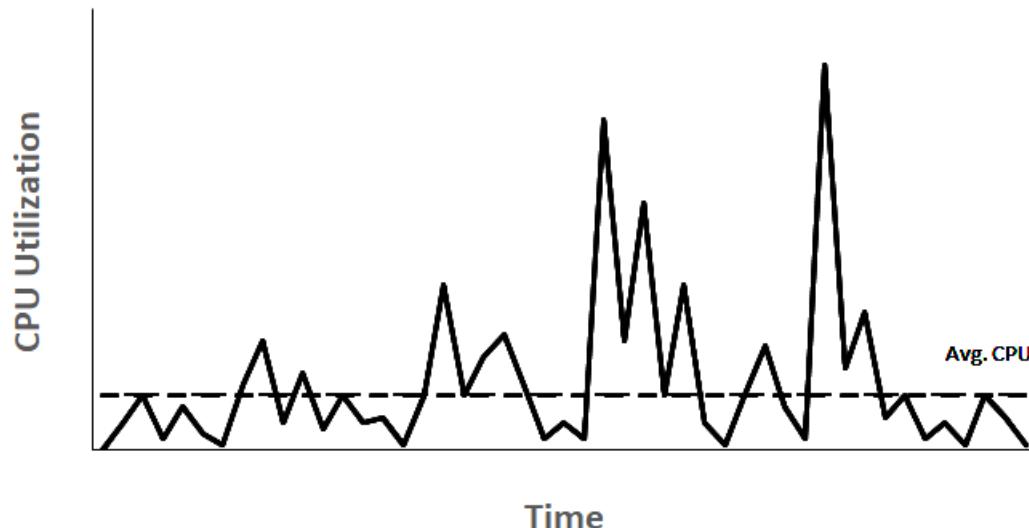
- Para obter a melhor performance de suas instâncias M6i, certifique-se de que elas tenham o driver ENA versão 2.2.3 ou posterior. Usar um driver ENA anterior à versão 2.0.0 com essas instâncias causará falhas no anexo da interface de rede. As AMIs a seguir têm driver ENA compatível.
 - AMI do Windows da AWS a partir de maio de 2021 ou posterior
- As instâncias criadas no Sistema Nitro oferecem suporte a, no máximo, 28 anexos, incluindo interfaces de rede, volumes do EBS e volumes de armazenamento de instâncias do NVMe. Para obter mais informações, consulte [Limites de volumes do Sistema Nitro \(p. 1507\)](#).
- Executar uma instância bare metal inicializa o servidor subjacente, o que inclui a verificação de todos os componentes de hardware e firmware. Isso significa que pode levar 20 minutos a partir do momento em que a instância entra no estado de execução até que ela se torne disponível na rede.

- Para anexar ou separar volumes do EBS ou interfaces de rede secundárias de uma instância bare metal, é necessário ter suporte PCIe hotplug nativo.
- As instâncias bare metal usam um dispositivo serial baseado em PCI em vez de um dispositivo serial baseado em porta de E/S. O kernel Linux upstream e as AMIs mais recentes do Amazon Linux suportam este dispositivo. As instâncias bare metal também fornecem uma tabela ACPI SPCR para permitir que o sistema use automaticamente o dispositivo serial baseado em PCI. As AMIs do Windows mais recentes usam automaticamente o dispositivo serial baseado em PCI.
- Existe um limite sobre o número total de instâncias que você pode executar em uma região e limites adicionais sobre alguns tipos de instância. Para obter mais informações, consulte [Quantas instâncias posso executar no Amazon EC2?](#) nas perguntas frequentes do Amazon EC2.

Instâncias expansíveis

Muitas workloads de uso geral não estão, em média, ocupadas e não exigem alto nível de performance da CPU sustentada. O gráfico a seguir ilustra a utilização da CPU para muitas workloads comuns executadas por clientes na Nuvem AWS hoje.

Many common workloads look like this



Essas workloads de utilização de CPU de baixa a moderada causam desperdício de ciclos de CPU e, consequentemente, você paga por mais do que usa. Para superar isso, é possível aproveitar as instâncias de uso geral expansíveis com baixo custo, que são as instâncias T.

A família de instâncias T fornece performance de CPU de linha de base com capacidade de intermitência acima da linha de base a qualquer momento, pelo tempo que for necessário. A CPU de linha de base é definida para atender às necessidades da maioria das workloads de uso geral, inclusive microsserviços de grande escala, servidores Web, bancos de dados pequenos e médios, registro em log de dados, repositórios de código, desktops virtuais, ambientes de desenvolvimento e teste e aplicações essenciais aos negócios. As instâncias T oferecem um equilíbrio de recursos de computação, memória e rede e fornecem a maneira mais econômica de executar um amplo espectro de aplicações de uso geral que têm uso de CPU de baixo a moderado. Podem economizar até 15% em custos, quando comparadas às instâncias M, e podem gerar ainda mais economia com tamanhos de instância menores e mais econômicas, oferecendo até 2 vCPUs e 0,5 GiB de memória. Os tamanhos de instância T menores, como nano, micro, pequeno e médio, são adequados para workloads que precisam de uma pequena quantidade de memória e não esperam alto uso da CPU.

Tipos de instância do EC2 expansíveis

As instâncias do EC2 com capacidade de intermitências consistem em tipos de instância T3a e T3 e nos tipos de instância T2 da geração anterior.

Os tipos de instância T4g são a geração mais recente de instâncias expansíveis. Fornecem o melhor preço por performance e o menor custo entre todos os tipos de instância do EC2. Os tipos de instância T4g são alimentados por processadores [AWS Graviton2](#) baseados em Arm com amplo suporte ao ecossistema de fornecedores de sistemas operacionais, fornecedores de software independentes e serviços e aplicações da AWS.

A tabela a seguir resume as principais diferenças entre os tipos de instância expansível.

Type	Descrição	Família de processadores
Última geração		
T4g	Tipo de instância do EC2 de menor custo com relação preço/performance até 40% mais alta e custos 20% menores em relação às T3	Processadores AWS Graviton2 com núcleos Arm Neoverse N1
T3a	Instâncias baseadas em x86 de menor custo com custos 10% mais baixos em relação às instâncias T3	Processadores AMD EPYC de 1.ª geração
T3	Melhor relação preço/performance de pico para workloads x86 com preço/performance até 30% mais baixos em relação às instâncias T2 da geração anterior	Intel Xeon escalável (processadores Skylake, Cascade Lake)
Geração anterior		
T2	Instâncias expansíveis da geração anterior	Processadores Intel Xeon

Para obter mais informações sobre o preço de instâncias e outras especificações, consulte [Preços do Amazon EC2](#) e [Tipos de instância do Amazon EC2](#).

Se sua conta tiver menos de 12 meses de vida, você poderá usar uma instância `t2.micro` gratuitamente (ou uma instância `t3.micro` em regiões em que `t2.micro` estiver indisponível) em determinados limites de uso. Para obter mais informações, consulte [Nível gratuito da AWS](#).

Opções de compra compatíveis com instâncias T

- On-Demand Instances
- Reserved Instances
- Instâncias dedicadas (apenas T3)
- Hosts dedicados (apenas T3, apenas no modo `standard`)
- Spot Instances

Para obter mais informações, consulte [Opções de compra de instância \(p. 253\)](#).

Tópicos

- [Práticas recomendadas \(p. 171\)](#)
- [Principais conceitos e definições para instâncias expansíveis \(p. 171\)](#)
- [Modo ilimitado de instâncias expansíveis \(p. 177\)](#)
- [Modo padrão de instâncias expansíveis \(p. 185\)](#)
- [Trabalhar com instâncias expansíveis \(p. 195\)](#)
- [Monitorar seus créditos da CPU \(p. 201\)](#)

Práticas recomendadas

Siga estas melhores práticas para obter o benefício máximo com as instâncias expansíveis.

- Verifique se o tamanho da instância escolhido ultrapassa os requisitos mínimos de memória do sistema operacional e das aplicações. Os sistemas operacionais com interfaces gráficas de usuário que consomem memória e recursos de CPU significativos (por exemplo, o Windows) podem exigir um tamanho de instância t3.micro, ou maior, para muitos casos de uso. À medida que os requisitos de memória e de CPU de sua workload aumentam, você tem a flexibilidade nas instâncias T para escalar para tamanhos de instâncias maiores do mesmo tipo ou selecionar outro tipo de instância.
- Habilite o [AWS Compute Optimizer](#) para sua conta e verifique as recomendações do Compute Optimizer para sua workload. O Compute Optimizer pode ajudar a avaliar se as instâncias devem ser ampliadas para melhorar a performance ou reduzidas para economizar custos.
- Para requisitos adicionais, consulte [Notas de release \(p. 168\)](#).

Principais conceitos e definições para instâncias expansíveis

Os tipos de instância do Amazon EC2 tradicionais fornecem recursos fixos de CPU, enquanto as instâncias expansíveis fornecem um nível de linha de base de CPU com capacidade para expandir o uso de CPU acima desse nível da linha de base. Isso garante que você pague somente pela CPU de linha de base, além dos usos adicionais de CPU de expansão, resultando em custos de computação mais baixos. O uso de linha de base e a capacidade de intermitência são governados por créditos de CPU. As instâncias expansíveis são os únicos tipos de instância que usam créditos para uso de CPU.

Cada instância expansível ganha crédito continuamente quando permanece abaixo da linha de base da CPU e gasta créditos continuamente quando expande acima da linha de base. A quantidade de créditos obtidos ou gastos depende do uso da CPU da instância:

- Se a utilização da CPU for maior do que linha de base, os créditos gastos serão maiores do que os créditos obtidos.
- Se a utilização da CPU for igual à linha de base, os créditos obtidos serão iguais aos créditos gastos.
- Se a utilização da CPU for menor do que linha de base, os créditos gastos serão maiores do que os créditos obtidos.

Quando os créditos obtidos são maiores do que os créditos gastos, a diferença é chamada de créditos acumulados, que podem ser usados posteriormente para expandir acima da utilização da CPU de linha de base. Da mesma forma, quando os créditos gastos são maiores do que créditos obtidos, o comportamento da instância depende do modo de configuração de crédito (modo padrão ou modo ilimitado).

No modo padrão, quando os créditos gastos são maiores do que os créditos obtidos, a instância usa os créditos acumulados para expandir acima da utilização da CPU de linha de base. Se não houver mais créditos acumulados, a instância se reduzirá gradualmente à utilização da CPU de linha de base e não poderá expandir acima da linha de base até acumular mais créditos.

No modo ilimitado, se a instância expandir acima da utilização da CPU de linha de base, a instância usará primeiro os créditos acumulados para expandir. Se não houver mais créditos acumulados, a instância

gastará créditos excedentes para expandir. Quando sua utilização de CPU ficar abaixo da linha de base, ela usará os créditos de CPU que ela ganhar para pagar os créditos excedentes gastos anteriormente. A capacidade de ganhar créditos de CPU para pagar créditos excedentes permite que o Amazon EC2 mantenha a média de utilização de CPU de uma instância em um período de 24 horas. Se o uso médio da CPU durante um período de 24 horas excede a linha de base, a instância será cobrada pelo uso adicional em uma taxa adicional fixa por hora de vCPU.

Tópicos

- [Principais conceitos e definições \(p. 172\)](#)
- [Ganhe créditos de CPU \(p. 174\)](#)
- [Taxa de ganhos de créditos de CPU \(p. 176\)](#)
- [Limite de acúmulo de créditos de CPU \(p. 176\)](#)
- [Duração dos créditos de CPU acumulados \(p. 176\)](#)
- [Utilização da linha de base \(p. 177\)](#)

Principais conceitos e definições

Os principais conceitos e definições a seguir são aplicáveis a instâncias expansíveis.

Utilização da CPU

Utilização de CPU é o percentual de unidades de processamento EC2 alocadas que estão em uso na instância no momento. Essa métrica mede a porcentagem de ciclos de CPU alocados que estão sendo utilizados em uma instância. A métrica CPU Utilization do CloudWatch mostra o uso da CPU por instância e não o uso da CPU por núcleo. A especificação de CPU de linha de base de uma instância também se baseia no uso da CPU por instância. Para medir a utilização da CPU usando o AWS Management Console ou a AWS CLI, consulte [Obter estatísticas para uma instância específica \(p. 914\)](#).

Crédito da CPU

Uma unidade de VCPU-time.

Exemplos:

1 crédito de CPU = 1 vCPU * 100% de utilização * 1 minuto.

1 crédito de CPU = 1 vCPU * 50% de utilização * 2 minutos

1 crédito de CPU = 2 vCPUs * 25% de utilização * 2 minutos

Utilização da linha de base

A utilização da linha de base é o nível no qual a CPU pode ser utilizada para um saldo de crédito líquido de zero, quando o número de créditos de CPU que estão sendo obtidos corresponde ao número de créditos de CPU que estão sendo usados. A utilização da linha de base também é conhecida como a linha de base. A utilização da linha de base é expressa como uma porcentagem da utilização da vCPU, que é calculada da seguinte forma: % da utilização da linha de base = (número de créditos ganhos/número de vCPUs)/60 minutos

Créditos ganhos

Créditos obtidos continuamente por uma instância quando ela está em execução.

Número de créditos ganhos por hora = % de utilização da linha de base * número de vCPUs * 60 minutos

Exemplo:

Um t3.nano com 2 vCPUs e utilização de linha de base de 5% ganha 6 créditos por hora, calculados da seguinte forma:

$$2 \text{ vCPUs} * 5\% \text{ da linha de base} * 60 \text{ minutos} = 6 \text{ créditos por hora}$$

Créditos gastos ou usados

Créditos usados continuamente por uma instância quando ela está em execução.

$$\text{Créditos de CPU gastos por minuto} = \text{Número de vCPUs} * \text{utilização da CPU} * 1 \text{ minuto}$$

Créditos acumulados

Créditos de CPU que não são gastos quando uma instância usa menos créditos do que o necessário para a utilização da linha de base. Em outras palavras, créditos acumulados = (Créditos obtidos - Créditos usados) abaixo da linha de base.

Exemplo:

Se um t3.nano estiver sendo executado com 2% de utilização da CPU, que está abaixo de sua linha de base de 5% por uma hora, os créditos acumulados serão calculados da seguinte forma:

$$\text{Créditos de CPU acumulados} = (\text{Créditos obtidos por hora} - \text{Créditos usados por hora}) = 6 - 2 \text{ vCPUs} * 2\% \text{ de utilização da CPU} * 60 \text{ minutos} = 6 - 2,4 = 3,6 \text{ créditos acumulados por hora}$$

Límite de acúmulo de créditos

Depende do tamanho da instância, mas em geral é igual ao número máximo de créditos obtidos em 24 horas.

Exemplo:

Para t3.nano, o limite de crédito acumulado = $24 * 6 = 144$ créditos

Créditos de execução

Aplicável somente a instâncias T2 configuradas para o modo padrão. Os créditos de inicialização são um número limitado de créditos de CPU alocados para uma nova instância T2, de modo que, quando iniciada no modo padrão, possa expandir acima da linha de base.

Créditos excedentes

Créditos que são gastos por uma instância após esgotar o saldo de crédito acumulado. Os créditos excedentes são projetados para instâncias intermitentes para sustentar alta performance por um longo período e são usados somente no modo ilimitado. O saldo de créditos excedentes é usado para determinar quantos créditos foram usados pela instância para expandir no modo ilimitado.

Modo padrão

Modo de configuração de crédito, que permite que uma instância se expanda acima da linha de base, gastando créditos acumulados no saldo de crédito.

Modo ilimitado

Modo de configuração de crédito, que permite que uma instância se expanda acima da linha de base, sustentando alta utilização da CPU por qualquer período, sempre que necessário. O preço por hora da instância cobre automaticamente todos os picos de uso da CPU se a utilização média de CPU da instância for igual ou menor que a linha de base durante um período contínuo de 24 horas ou durante a vida útil da instância, o que for menor. Se a instância funcionar com maior utilização de CPU por um período prolongado, ela poderá fazer isso por uma taxa adicional uniforme por hora de vCPU.

A tabela a seguir resume as principais diferenças de crédito entre os tipos de instância expansível.

Type	Tipo de créditos de CPU compatíveis	Modos de configuração de crédito	Vida útil de créditos de CPU acumulados entre a inicialização e a interrupção da instância
Última geração			
T4g	Créditos obtidos, créditos acumulados, créditos gastos, créditos excedentes (somente no modo ilimitado)	Padrão, ilimitado (padrão)	7 dias (os créditos permanecem por 7 dias após a interrupção de uma instância)
T3a	Créditos obtidos, créditos acumulados, créditos gastos, créditos excedentes (somente no modo ilimitado)	Padrão, ilimitado (padrão)	7 dias (os créditos permanecem por 7 dias após a interrupção de uma instância)
T3	Créditos obtidos, créditos acumulados, créditos gastos, créditos excedentes (somente no modo ilimitado)	Padrão, ilimitado (padrão)	7 dias (os créditos permanecem por 7 dias após a interrupção de uma instância)
Geração anterior			
T2	Créditos obtidos, créditos acumulados, Créditos gastos, créditos de inicialização (somente no modo padrão), créditos excedentes (somente no modo ilimitado)	Standard (padrão), ilimitado	0 dias (os créditos são perdidos quando uma instância é interrompida)

Note

O modo ilimitado não é compatível com instâncias T3 que são iniciadas em um Host Dedicado.

Ganhe créditos de CPU

Cada instância expansível ganha continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos de CPU por hora, de acordo com o tamanho da instância. O processo de contabilidade de se os créditos são acumulados ou gastos também ocorre em uma resolução em nível de milissegundo, portanto, você não precisa se preocupar com gastos excessivos de créditos de CPU. Uma intermitência curta da CPU usa uma pequena fração de um crédito de CPU.

Se uma instância expansível usar menos recursos de CPU do que o necessário para o uso de linha de base (como, por exemplo, quando está inativa), os créditos de CPU não gastos serão acumulados no saldo de créditos de CPU. Se uma instância expansível precisar de intermitência acima do nível do uso da linha de base, ela gastará os créditos acumulados. Quanto mais créditos a instância expansível acumular, mais tempo de intermitência ela poderá ter acima da linha de base quando mais uso de CPU for necessário.

A tabela a seguir lista os tipos de instância expansível, a taxa na qual os créditos de CPU são ganhos por hora, o número máximo de créditos de CPU ganhos que uma instância pode acumular, o número de

vCPUs por instância e o uso da linha de base como uma porcentagem do total de um núcleo (usando uma única vCPU).

Tipo de instância	Créditos de CPU ganhos por hora	Máximo de créditos obtidos que podem ser acumulados*	vCPUs***	Utilização da linha de base por vCPU
T2				
t2.nano	3	72	1	5%
t2.micro	6	144	1	10%
t2.small	12	288	1	20%
t2.medium	24	576	2	20%**
t2.large	36	864	2	30%**
t2.xlarge	54	1296	4	22,5%**
t2.2xlarge	81.6	1958.4	8	17%**
T3				
t3.nano	6	144	2	5%**
t3.micro	12	288	2	10%**
t3.small	24	576	2	20%**
t3.medium	24	576	2	20%**
t3.large	36	864	2	30%**
t3.xlarge	96	2304	4	40%**
t3.2xlarge	192	4608	8	40%**
T3a				
t3a.nano	6	144	2	5%**
t3a.micro	12	288	2	10%**
t3a.small	24	576	2	20%**
t3a.medium	24	576	2	20%**
t3a.large	36	864	2	30%**
t3a.xlarge	96	2304	4	40%**
t3a.2xlarge	192	4608	8	40%**

* O número de créditos que podem ser acumulados é equivalente ao número de créditos que podem ser obtidos em um período de 24 horas.

**A porcentagem de utilização da linha de base na tabela é por vCPU. Em CloudWatch, a utilização da CPU é exibida por vCPU. Por exemplo, a utilização de CPU para uma instância t3.large que

opera no nível de linha de base é mostrada como 30% nas métricas de CPU do CloudWatch. Para obter informações sobre como calcular a utilização da linha de base, consulte [Utilização da linha de base \(p. 177\)](#).

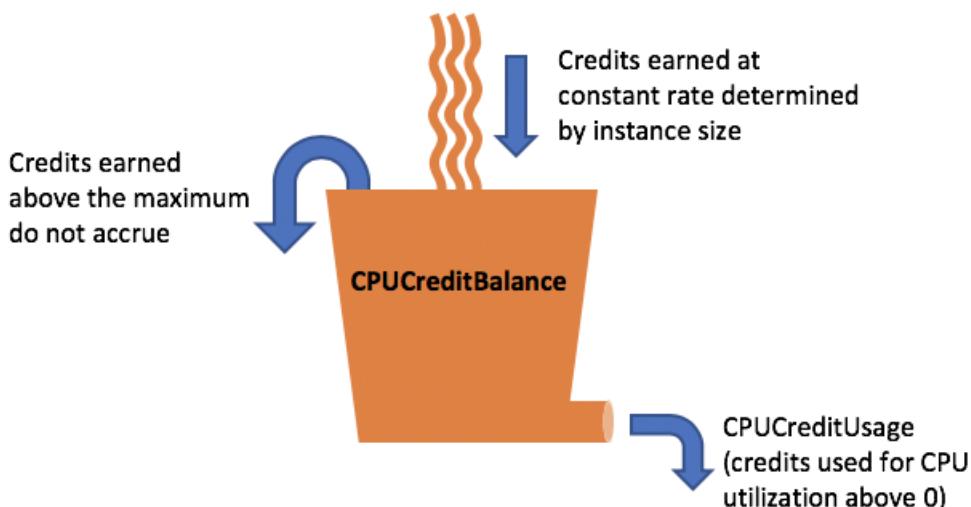
*** Cada vCPU é uma thread de um núcleo Intel Xeon ou de um núcleo AMD EPYC, exceto para instâncias T2 .

Taxa de ganhos de créditos de CPU

O número de créditos de CPU ganhos por hora é determinado pelo tamanho da instância. Por exemplo, t3.nano ganha seis créditos por hora, enquanto t3.small ganha 24 créditos por hora. A tabela anterior lista a taxa de ganhos de crédito de todas as instâncias.

Límite de acúmulo de créditos de CPU

Embora os créditos obtidos nunca expirem em uma instância em execução, há um limite para o número de créditos obtidos que uma instância pode acumular. O limite é determinado pelo limite de saldo de créditos de CPU. Após o limite ser atingido, todos os créditos novos que foram ganhos serão rejeitados, como indicado na imagem a seguir. O bucket completo indica o limite de saldo de créditos de CPU, e o spillover indica os créditos ganhos recentemente que excedem o limite.



O limite de saldo de créditos de CPU difere para cada tamanho de instância. Por exemplo, uma instância t3.micro pode acumular no máximo 288 créditos no saldo de créditos de CPU. A tabela anterior lista o número máximo de créditos ganhos que cada instância pode acumular.

As instâncias T2 padrão também ganham créditos de execução. Os créditos de execução não são contabilizados para o limite de saldo de créditos de CPU. Se uma instância T2 não gastar os créditos de execução e permanecer ociosa por um período de 24 horas, acumulando os créditos obtidos, seu saldo de créditos de CPU serão exibidos como acima do limite. Para obter mais informações, consulte [Créditos de execução \(p. 186\)](#).

As instâncias T3a e T3 não ganham créditos de inicialização. Essas instâncias são executadas como `unlimited` por padrão e, portanto, podem apresentar intermitência imediatamente desde o início, sem nenhum crédito de execução. Instâncias T3 iniciadas em um lançamento de Host Dedicado como `standard` por padrão, o modo `>unlimited` não é compatível para instâncias T3 em um Host Dedicado.

Duração dos créditos de CPU acumulados

Os créditos de CPU de uma instância em execução não expiram.

Para T2, o saldo de créditos de CPU não persiste entre interrupções e inicializações da instância. Se você interromper uma instância T2, a instância perderá todos os créditos acumulados.

Para T3a e T3, o saldo de créditos de CPU persiste durante sete dias após uma instância ser interrompida, e os créditos são perdidos após esse período. Se você iniciar a instância dentro de sete dias, nenhum crédito será perdido.

Para obter mais informações, consulte [CPU Credit Balance na Tabela de métricas do CloudWatch \(p. 201\)](#).

Utilização da linha de base

A utilização da lista de base é o nível no qual a CPU pode ser utilizada para um saldo de crédito líquido igual a zero, quando o número de créditos de CPU obtidos correspondem ao número de créditos de CPU usados. A utilização da linha de base também é conhecida como a linha de base.

A utilização da linha de base é expressa como uma porcentagem da utilização da vCPU, que é calculada da seguinte forma:

$(\text{number of credits earned}/\text{number of vCPUs})/60 \text{ minutes} = \% \text{ baseline utilization}$

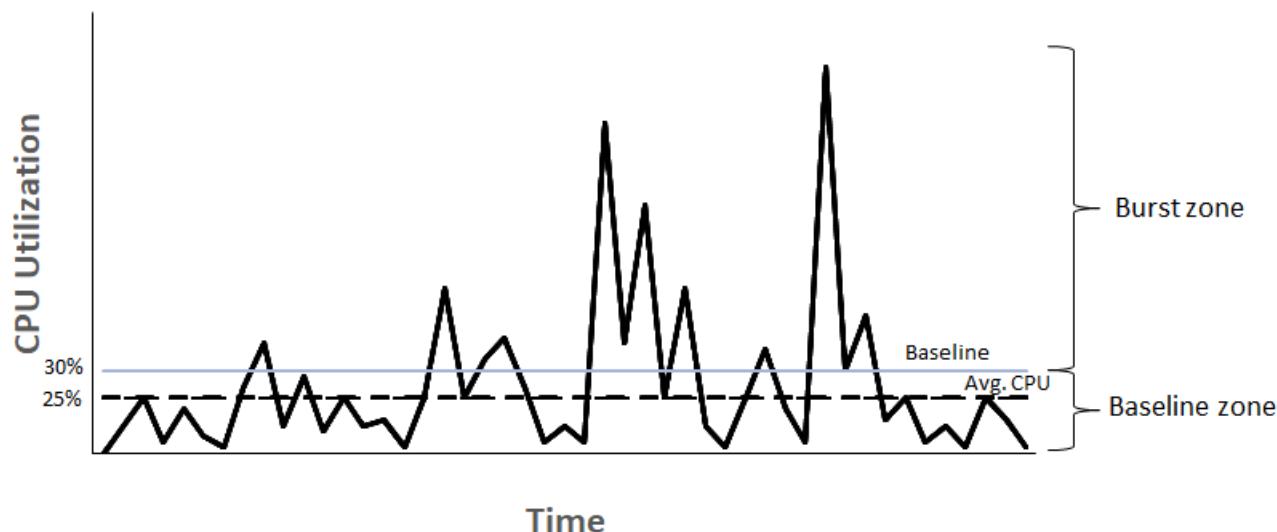
Por exemplo, uma instância t3.nano, com 2 vCPUs, ganha 6 créditos por hora, resultando em uma utilização de linha de base de 5%, que é calculada da seguinte forma:

$(6 \text{ credits earned}/2 \text{ vCPUs})/60 \text{ minutes} = 5\% \text{ baseline utilization}$

Uma instância t3.xlarge, com 4 vCPUs, ganha 96 créditos por hora, resultando em uma utilização de linha de base de 40% $((96/4)/60)$.

O gráfico a seguir fornece um exemplo de t3.large com utilização média da CPU abaixo da linha de base.

Example of t3.large



Modo ilimitado de instâncias expansíveis

Uma instância expansível configurada como `unlimited` pode sustentar alta utilização de CPU por qualquer período, sempre que necessário. O preço por hora da instância cobre automaticamente todos os

picos de uso da CPU se a utilização média de CPU da instância for igual ou menor que a linha de base durante um período contínuo de 24 horas ou durante a vida útil da instância, o que for menor.

Na grande maioria das workloads de uso geral, as instâncias configuradas como `unlimited` fornecem uma performance ampla sem encargos adicionais. Se a instância funcionar com maior utilização de CPU por um período prolongado, ela poderá fazer isso por uma taxa adicional uniforme por hora de vCPU. Para obter informações sobre preços, consulte a [definição de preço do Amazon EC2](#) e [definição de preço do modo ilimitado T2/T3/T4](#).

Se você usar uma instância `t2.micro` ou `t3.micro` na oferta [AWS Nível gratuito da](#) e usá-la no modo `unlimited`, poderão ser aplicados encargos se a sua utilização média durante um período contínuo de 24 horas exceder a [utilização de linha de base \(p. 177\)](#) da instância.

As instâncias T3a e T3 são iniciadas como `unlimited` por padrão. Se a média de uso de CPU em um período de 24 horas exceder a linha de base, você incorrerá em cobranças por créditos excedentes. Se você executar Instâncias spot como `unlimited` e planejar usá-las imediatamente e por um curto período, sem tempo ocioso para acumular créditos de CPU, serão cobrados créditos excedentes. Recomendamos iniciar as instâncias spot no modo [padrão \(p. 185\)](#) para evitar custos mais altos. Para obter mais informações, consulte [Os créditos excedentes podem gerar cobranças \(p. 181\)](#) e [Instâncias expansíveis \(p. 348\)](#).

Note

Instâncias T3 iniciadas em um lançamento de Host Dedicado como `standard` por padrão, o modo `unlimited` não é compatível para instâncias T3 em um Host Dedicado.

Tópicos

- [Conceitos do modo ilimitado \(p. 178\)](#)
 - [Como funcionam as instâncias expansíveis \(p. 178\)](#)
 - [Quando usar o modo ilimitado versus CPU fixa \(p. 179\)](#)
 - [Os créditos excedentes podem gerar cobranças \(p. 181\)](#)
 - [Nenhum crédito de execução para T2 ilimitada \(p. 181\)](#)
 - [Ativar modo ilimitado \(p. 182\)](#)
 - [O que acontece com os créditos quando é feita alternância de ilimitada para padrão \(p. 182\)](#)
 - [Monitorar uso de crédito \(p. 182\)](#)
- [Exemplos de modo ilimitado \(p. 182\)](#)
 - [Exemplo 1: explicar o uso de créditos com T3 ilimitada \(p. 182\)](#)
 - [Exemplo 2: explicar o uso de créditos com T2 ilimitada \(p. 184\)](#)

[Conceitos do modo ilimitado](#)

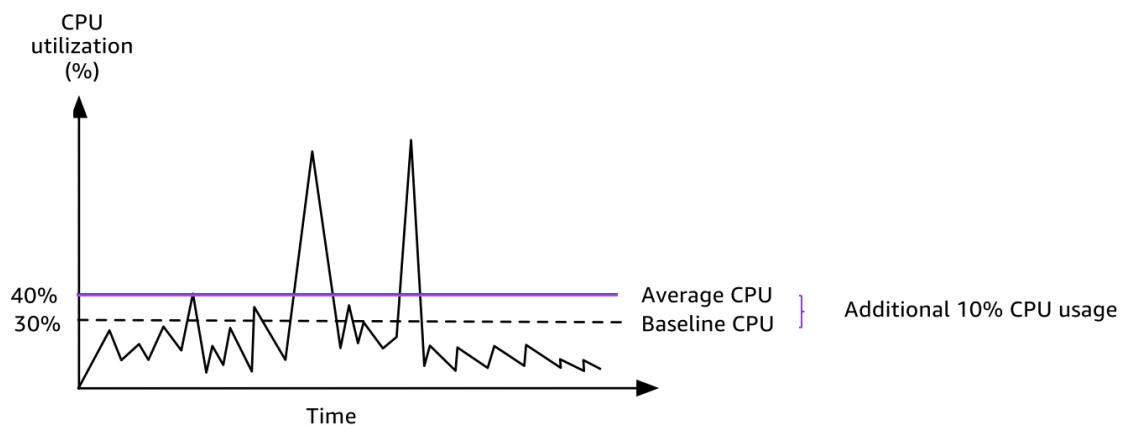
O modo `unlimited` é uma opção de configuração de crédito para instâncias expansíveis. Ele pode ser habilitado ou desabilitado a qualquer momento para uma instância interrompida ou em execução. Você pode definir `unlimited` como a opção de crédito padrão no nível da conta por região da AWS, por família de instâncias expansíveis, para que todas as novas instâncias de performance com capacidade de intermitência na conta sejam executadas usando a opção de crédito padrão.

[Como funcionam as instâncias expansíveis](#)

Se uma instância expansível configurada como `unlimited` esgota seu crédito de CPU, ela pode gastar créditos excedentes para ter intermitência acima da [linha de base \(p. 177\)](#). Quando sua utilização de CPU ficar abaixo da linha de base, ela usará os créditos de CPU que ela ganhar para pagar os créditos excedentes gastos anteriormente. A capacidade de ganhar créditos de CPU para pagar créditos excedentes permite que o Amazon EC2 mantenha a média de utilização de CPU de uma instância em

um período de 24 horas. Se o uso médio da CPU durante um período de 24 horas exceder a lista de referência, a instância será cobrada pelo uso adicional em uma [taxa adicional fixa](#) por hora de vCPU.

O gráfico a seguir mostra o uso da CPU de um t3.large. A utilização da CPU de linha de base para um t3.large é 30%. Se a instância for executada com 30% de utilização da CPU ou menos, em média, durante um período de 24 horas, não haverá cobrança adicional porque o custo já está coberto pelo preço por hora da instância. No entanto, se a instância for executada com 40% de utilização da CPU, em média, durante um período de 24 horas, conforme mostrado no gráfico, a instância será cobrada pelo uso adicional de 10% da CPU em uma [taxa adicional fixa](#) por hora de vCPU.



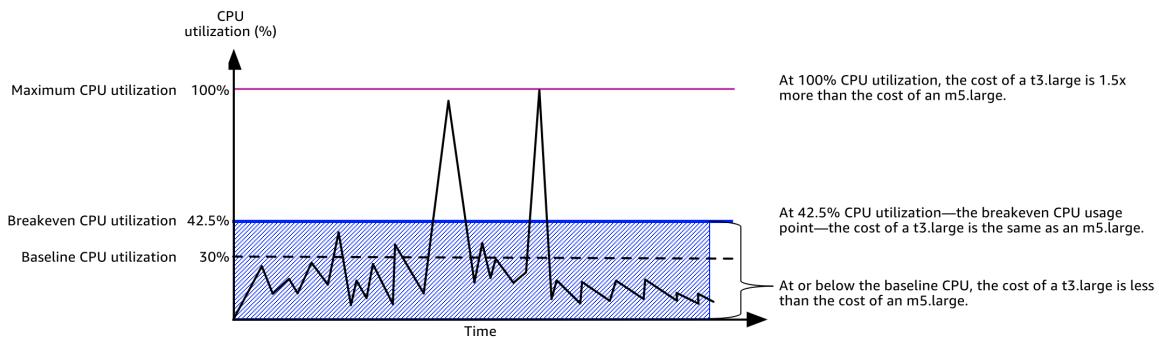
Para obter mais informações sobre a utilização da linha de base por vCPU para cada tipo de instância e quantos créditos cada tipo de instância recebe, consulte a [tabela de créditos](#) (p. 175).

Quando usar o modo ilimitado versus CPU fixa

Ao determinar se você deve usar uma instância expansível no modo `unlimited`, como T3, ou uma instância de performance fixa, como M5, você precisa determinar o uso da CPU de equilíbrio. O uso da CPU de equilíbrio para uma instância expansível é o ponto em que uma instância expansível custa o mesmo que uma instância de performance fixa. O uso da CPU de equilíbrio ajuda a determinar o seguinte:

- Se o uso médio da CPU em um período de 24 horas estiver no uso de CPU de equilíbrio ou abaixo dele, use uma instância expansível no modo `unlimited` para que você possa se beneficiar do preço mais baixo de uma instância expansível enquanto obtém a mesma performance de uma instância de performance fixa.
- Se o uso médio da CPU durante um período de 24 horas estiver acima do uso de CPU de equilíbrio, a instância expansível custará mais do que a instância de performance fixa de tamanho equivalente. Se uma instância T3 apresentar uma intermitência contínua para 100% da CPU, você acabará pagando aproximadamente 1,5 vezes o preço de uma instância M5 de tamanho equivalente.

O gráfico a seguir mostra o ponto de uso da CPU de equilíbrio em que um t3.large custa o mesmo que um m5.large. O ponto de uso da CPU de equilíbrio para um t3.large é 42,5%. Se o uso médio da CPU estiver em 42,5%, o custo de executar o t3.large é o mesmo que um m5.large, e é mais caro se o uso médio da CPU estiver acima de 42,5%. Se a workload precisar de menos de 42,5% do uso médio da CPU, você poderá se beneficiar do preço mais baixo do t3.large ao obter a mesma performance de um m5.large.



A tabela a seguir mostra como calcular o limite de uso da CPU de equilíbrio para que você possa determinar quando é mais barato usar uma instância expansível no modo *unlimited* ou uma instância de performance fixa. As colunas na tabela são rotuladas de A a K.

Tipo de instância	vCPUs	Preço*/ hora de T3	Preço*/ hora de M5	Diferença de preço	Utilização da linha base	Cobrança por hora de vCPU base	Cobrança por minuto de vCPU excedente	Mais minutos de intermitência disponíveis	% de CPU adicional	% de CPU de equilíbrio
									T3 por vCPU excedente (%)	J = (I / 60) / B
A	B	C	D	E = D - C	F	G	H = G / 60	I = E / H	J = (I / 60) / B	K = F + J
t3.large	2	US\$ 0,096	US\$ 0,125	30%	0,05	US\$ 0,000833		15	12,5%	42,5%
		0,0835								

*O preço é baseado no us-east-1 e no SO Linux.

A tabela fornece as seguintes informações:

- A coluna A mostra o tipo de instância, **t3.large**.
- A coluna B mostra o número de vCPUs para o **t3.large**.
- A coluna C mostra o preço de um **t3.large** por hora.
- A coluna D mostra o preço de um **m5.large** por hora.
- A coluna E mostra a diferença de preço entre o **t3.large** e o **m5.large**.
- A coluna F mostra a utilização da linha de base por vCPU do **t3.large**, que é 30%. Na linha de base, o custo por hora da instância abrange o custo do uso da CPU.
- A coluna G mostra a **taxa adicional fixa** por hora de vCPU em que uma instância é cobrada, se apresentar uma intermitência em 100% da CPU depois de ter esgotado seus créditos ganhos.
- A coluna H mostra a **taxa adicional fixa** por minuto de vCPU em que uma instância é cobrada, se apresentar uma intermitência em 100% da CPU depois de ter esgotado seus créditos ganhos.
- A coluna I mostra o número de minutos adicionais que o **t3.large** pode apresentar uma intermitência por hora para 100% da CPU pagando o mesmo preço por hora que um **m5.large**.
- A coluna J mostra o uso adicional da CPU (em %) ao longo da linha de base em que a instância pode apresentar uma intermitência enquanto paga o mesmo preço por hora que um **m5.large**.

- A coluna K mostra o uso da CPU de equilíbrio (em%) em que o `t3.large` pode apresentar uma intermitência sem pagar mais do que o `m5.large`. Qualquer coisa acima disso, e o `t3.large` custará mais do que o `m5.large`.

A tabela a seguir mostra o uso da CPU de equilíbrio (em%) para os tipos de instância T3 em comparação com os tipos de instância M5 de tamanho semelhante.

Tipo de instância do T3	Uso da CPU de equilíbrio (em %) para T3 comparado a M5
<code>t3.large</code>	42,5%
<code>t3.xlarge</code>	52,5 %
<code>t3.2xlarge</code>	52,5 %

Os créditos excedentes podem gerar cobranças

Se a utilização média de CPU de um instância for igual ou inferior à linha de base, a instância não incorrerá encargos adicionais. Como uma instância ganha um [número máximo de créditos \(p. 175\)](#) em um período de 24 horas (por exemplo, uma instância `t3.micro` pode ganhar no máximo 288 créditos em um período de 24 horas), ela pode gastar créditos excedentes até esse limite máximo sem gerar uma cobranças imediatamente.

Contudo, se a utilização de CPU permanecer acima da linha de base, a instância não poderá obter créditos suficientes para pagar os créditos excedentes que ela gastou. Os créditos excedentes que não são pagos são cobrados a uma taxa adicional fixa por hora de vCPU. Para obter informações sobre a taxa, consulte a [definição de preço do modo ilimitado T2/T3/T4g](#).

Os créditos excedentes que foram gastos anteriormente são cobrados quando uma das seguintes situações ocorre:

- Os créditos excedentes ultrapassaram o [número máximo de créditos \(p. 175\)](#) que a instância pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora.
- A instância é interrompida ou encerrada.
- A instância é alterada de `unlimited` para `standard`.

Os créditos excedentes gastos são monitorados pela métrica CloudWatch do `CPUSurplusCreditBalance`. Os créditos excedentes cobrados são monitorados pela métrica CloudWatch do `CPUSurplusCreditsCharged`. Para obter mais informações, consulte [Métricas adicionais do CloudWatch para instâncias expansíveis \(p. 201\)](#).

Nenhum crédito de execução para T2 ilimitada

As instâncias T2 padrão recebem [créditos de execução \(p. 186\)](#), mas as instâncias T2 ilimitadas não as recebem. Uma instância T2 ilimitada pode apresentar intermitência acima da linha de base a qualquer momento, sem encargos adicionais, desde que sua utilização média de CPU seja igual ou inferior à linha de base em um período contínuo de 24 horas ou durante sua vida útil, o que for menor. Como tal, as instâncias T2 ilimitadas não requerem créditos de execução para atingir alta performance imediatamente após a execução.

Se uma instância T2 for alterada de `standard` para `unlimited`, todos os créditos de execução acumulados serão removidos do `CPUCreditBalance` antes do `CPUCreditBalance` restante ser transferido.

As instâncias T3a e T3 nunca recebem créditos de inicialização porque são compatíveis com o modo ilimitado. A configuração de crédito de modo ilimitado permite que as instâncias T4g, T3a e T3 usem o máximo de CPU necessário para expandir além da linha de base e pelo tempo necessário.

Ativar modo ilimitado

Você pode alterar de `unlimited` para `standard` e de `standard` para `unlimited` a qualquer momento em uma instância interrompida ou em execução. Para obter mais informações, consulte [Iniciar uma instância expansível como ilimitada ou padrão \(p. 196\)](#) e [Modificar a especificação de crédito de uma instância expansível \(p. 199\)](#).

Você pode definir `unlimited` como a opção de crédito padrão no nível da conta por região da AWS, por família de instâncias expansíveis, para que todas as novas instâncias de performance com capacidade de intermitência na conta sejam executadas usando a opção de crédito padrão. Para obter mais informações, consulte [Definir a especificação de crédito padrão para a conta \(p. 200\)](#).

É possível verificar se uma instância expansível está configurada como `unlimited` ou `standard` usando o console do Amazon EC2 ou a AWS CLI. Para obter mais informações, consulte [Exibir a especificação de crédito de uma instância expansível \(p. 198\)](#) e [Visualizar a especificação de crédito padrão \(p. 200\)](#).

O que acontece com os créditos quando é feita alternância de ilimitada para padrão

`CPUCreditBalance` é uma métrica do CloudWatch que controla o número de créditos que uma instância acumulou. `CPUSurplusCreditBalance` é uma métrica do CloudWatch que monitora o número de créditos excedentes que uma instância gastou.

Ao alterar uma instância configurada como `unlimited` para `standard`, ocorre o seguinte:

- O valor `CPUCreditBalance` permanece inalterado e é transferido.
- O valor `CPUSurplusCreditBalance` é cobrado imediatamente.

Quando uma instância `standard` é alterada para `unlimited`, ocorre o seguinte:

- O valor `CPUCreditBalance` que contém créditos ganhos acumulados é transferido.
- Para instâncias T2 padrão, todos os créditos de execução são removidos do valor `CPUCreditBalance`, e o valor `CPUCreditBalance` que contém os créditos ganhos acumulados é transferido.

Monitorar uso de crédito

Para verificar se a instância está gastando mais créditos do que a linha de base fornece, você pode usar as métricas do CloudWatch no monitoramento do uso e configurar alarmes horários para ser notificado sobre o uso de crédito. Para obter mais informações, consulte [Monitorar seus créditos da CPU \(p. 201\)](#).

Exemplos de modo ilimitado

Os seguintes exemplos explicam o uso de créditos para instâncias configuradas como `unlimited`.

Exemplos

- [Exemplo 1: explicar o uso de créditos com T3 ilimitada \(p. 182\)](#)
- [Exemplo 2: explicar o uso de créditos com T2 ilimitada \(p. 184\)](#)

Exemplo 1: explicar o uso de créditos com T3 ilimitada

Neste exemplo, você verá a utilização de CPU de uma instância t3.nano executada como `unlimited` e como ela gasta créditos ganhos e excedentes para sustentar a utilização de CPU.

A instância t3.nano ganha 144 créditos de CPU em um período contínuo de 24 horas, que ela pode resgatar para 144 minutos de uso de vCPU. Quando ela esgotar o saldo de créditos de CPU (representado pela métrica CloudWatch do CPUCreditBalance), poderá gastar os créditos de CPU—excedentes, que ela ainda não ganhou—, para ter intermitência durante o tempo que precisar. Como uma instância t3.nano ganha no máximo 144 créditos em um período de 24 horas, ela poderá gastar os créditos excedentes até esse limite máximo, sem ser cobrada imediatamente por isso. Se ela gastar mais de 144 créditos de CPU, será cobrada pela diferença no final da hora.

A intenção do exemplo, ilustrada pelo gráfico a seguir, é mostrar como uma instância pode apresentar intermitência usando créditos excedentes, mesmo após esgotar seu CPUCreditBalance. O fluxo de trabalho a seguir faz referência aos pontos numerados no gráfico:

P1 – às 0 horas no gráfico, a instância é executada como `unlimited` e começa a ganhar créditos imediatamente. A instância permanece inativa desde a sua execução (o uso da CPU é de 0%), e nenhum crédito é gasto. Todos os créditos não gastos são acumulados no saldo de crédito. Nas primeiras 24 horas, CPUCreditUsage é de 0, e o valor CPUCreditBalance atinge seu máximo de 144.

P2 – nas próximas 12 horas, a utilização de CPU é de 2,5%, que é abaixo da linha de base de 5%. A instância ganha mais créditos do que gasta, mas o valor CPUCreditBalance não pode exceder seu máximo de 144 créditos.

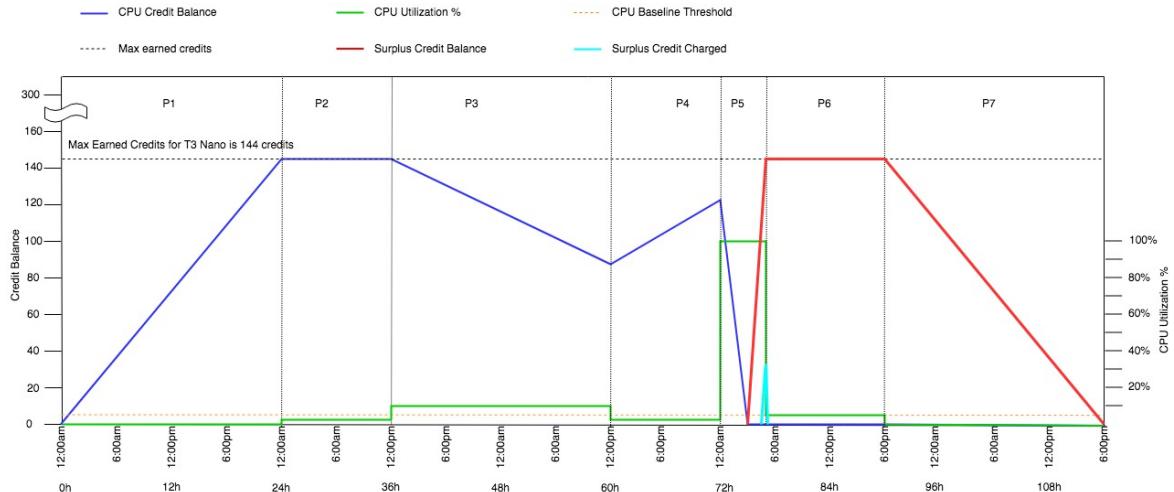
P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor CPUCreditBalance diminui para 86,4 créditos.

P4 – nas próximas 12 horas, a utilização de CPU diminui para 2,5% (abaixo da linha de base), o que exige um gasto de 36 créditos. Ao mesmo tempo, a instância ganha 72 créditos. A instância ganha mais créditos do que gasta, e o valor CPUCreditBalance aumenta para 122 créditos.

P5 – nas próximas 5 horas, a instância tem intermitência para 100% de utilização de CPU e gasta um total de 570 créditos para sustentar a intermitência. Após aproximadamente uma hora desse período, a instância esgota todo o CPUCreditBalance de 122 créditos e começa a gastar os créditos excedentes para sustentar o alto uso de CPU, totalizando 448 créditos excedentes nesse período ($570 - 122 = 448$). Quando o valor CPUSurplusCreditBalance atingir 144 créditos de CPU (o máximo que uma instância t3.nano pode ganhar em um período de 24 horas), todos os créditos excedentes gastos após esse período não poderão ser compensados por créditos ganhos. Os créditos excedentes gastos depois desse período totalizam 304 créditos ($448 - 144 = 304$), resultando em uma pequena cobrança adicional ao fim dessa hora para 304 créditos.

P6 – nas próximas 13 horas, a utilização de CPU é de 5%, (a linha de base). A instância ganha o número de créditos que gastar, sem precisar pagar por excessos do CPUSurplusCreditBalance. O valor CPUSurplusCreditBalance permanece em 144 créditos.

P7 – nas últimas 24 horas neste exemplo, a instância está inativa, e a utilização de CPU é de 0%. Durante esse período, a instância ganha 144 créditos, que usa para pagar o CPUSurplusCreditBalance.



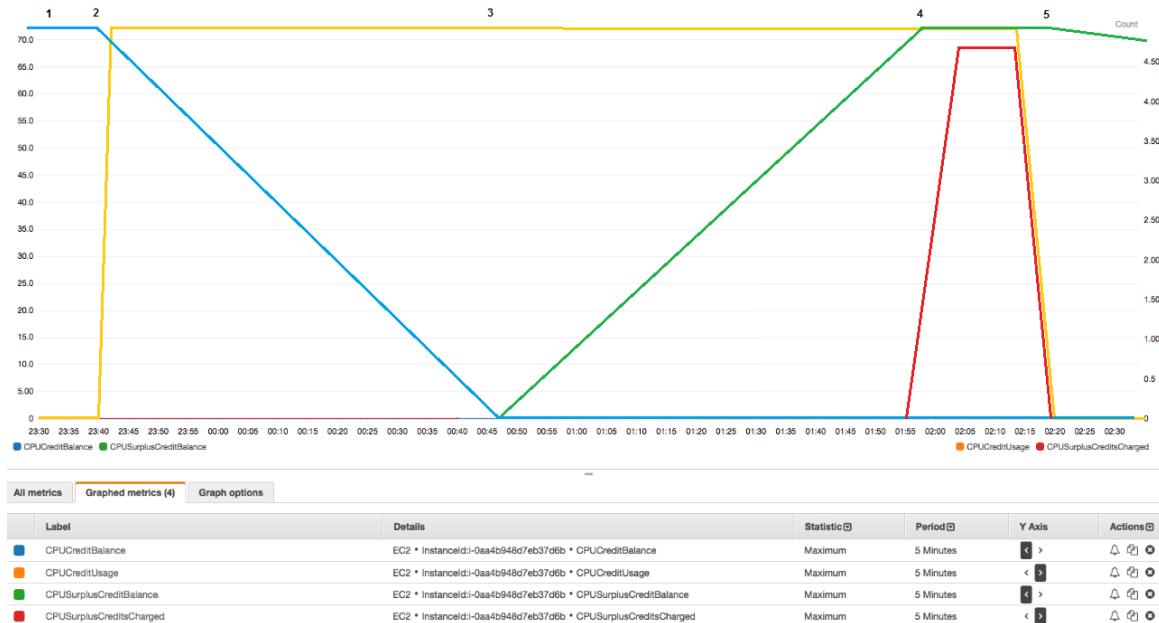
Exemplo 2: explicar o uso de créditos com T2 ilimitada

Neste exemplo, você verá a utilização de CPU de uma instância `t2.nano` executada como `unlimited` e como ela gasta créditos ganhos e excedentes para sustentar a utilização de CPU.

A instância `t2.nano` ganha 72 créditos de CPU em um período contínuo de 24 horas, que ela pode resgatar para 72 minutos de uso de vCPU. Quando ela esgotar o saldo de créditos de CPU (representado pela métrica CloudWatch do `CPUCreditBalance`), poderá gastar os créditos de CPU—excedentes, que ela ainda não ganhou—, para ter intermitência durante o tempo que precisar. Como uma instância `t2.nano` ganha no máximo 72 créditos em um período de 24 horas, ela poderá gastar os créditos excedentes até esse limite máximo, sem ser cobrada imediatamente por isso. Se ela gastar mais de 72 créditos de CPU, será cobrada pela diferença no final da hora.

A intenção do exemplo, ilustrada pelo gráfico a seguir, é mostrar como uma instância pode apresentar intermitência usando créditos excedentes, mesmo após esgotar seu `CPUCreditBalance`. Você pode supor que, no início de linha de tempo no gráfico, a instância tem um saldo de créditos acumulados igual ao número máximo de créditos que ela pode ganhar em 24 horas. O fluxo de trabalho a seguir faz referência aos pontos numerados no gráfico:

- 1 – Nos primeiros 10 minutos, `CPUCreditUsage` está em 0 e o valor `CPUCreditBalance` permanece no limite máximo de 72.
- 2 – Às 23H40, à medida que a utilização da CPU aumenta, a instância gasta os créditos de CPU e o valor `CPUCreditBalance` diminui.
- 3 – Por volta de 00h47, a instância esgota todo o seu `CPUCreditBalance` e começa a gastar os créditos excedentes para manter o alto uso da CPU.
- 4 – Os créditos excedentes são gastos até 01h55, quando o valor `CPUSurplusCreditBalance` atinge 72 créditos de CPU. Isso é igual ao limite máximo que uma instância `t2.nano` pode ganhar em um período de 24 horas. Qualquer crédito excedente gasto a partir daí não poderá ser compensado pelos créditos ganhos no período de 24 horas, o que resultará em uma pequena taxa adicional no final da hora.
- 5 – A instância continua a gastar os créditos excedentes até às 02h20. Nesse momento, a utilização da CPU cai abaixo da linha de base, e a instância começa a ganhar 3 créditos por hora (ou 0,25 crédito a cada 5 minutos), que ela usa para pagar o `CPUSurplusCreditBalance`. Quando o valor `CPUSurplusCreditBalance` reduz para 0, a instância começa a acumular créditos ganhos em seu `CPUCreditBalance` a 0,25 crédito a cada 5 minutos.



Cálculo da conta

Os créditos excedentes custam 0,096 USD por hora de vCPU. A instância gastou cerca de 25 créditos excedentes entre 01h55 e 02h20, o que equivale a 0,42 horas de vCPU.

As cobranças adicionais para essa instância são $0,42 \text{ hora de vCPU} \times 0,096 \text{ USD/hora de vCPU} = 0,04032 \text{ USD}$, arredondado para 0,04 USD.

Esta é a conta de final do mês desta instância T2 ilimitada:

Amazon Elastic Compute Cloud running Windows		
\$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	\$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
\$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	\$0.04

Você pode configurar alertas de pagamento para ser notificado a cada hora sobre quaisquer cobranças acumuladas e tomar providências, se necessário.

Modo padrão de instâncias expansíveis

Uma instância expansível configurada como `standard` é adequada para workloads com uma utilização média de CPU consistentemente abaixo da utilização de CPU de linha de base da instância. Para intermitências acima da linha de base, a instância gasta os créditos acumulados no seu saldo de créditos de CPU. Se a instância estiver ficando sem créditos acumulados, o uso de CPU será gradualmente reduzido para o nível da linha de base, para que a instância não experimente uma queda de performance acentuada quando o saldo de créditos de CPU acumulado se esgotar. Para obter mais informações, consulte [Principais conceitos e definições para instâncias expansíveis \(p. 171\)](#).

Tópicos

- [Conceitos do modo padrão \(p. 186\)](#)
 - [Como funcionam as instâncias expansíveis padrão \(p. 186\)](#)
 - [Créditos de execução \(p. 186\)](#)

- [Limites de crédito de execução \(p. 187\)](#)
- [Diferenças entre créditos de execução e créditos ganhos \(p. 187\)](#)
- [Exemplos de modo padrão \(p. 188\)](#)
 - [Exemplo 1: explicar o uso de créditos com T3 padrão \(p. 188\)](#)
 - [Exemplo 2: explicar o uso de créditos com T2 padrão \(p. 189\)](#)
 - Período 1: 1 a 24 horas (p. 190)
 - Período 2: 25 a 36 horas (p. 190)
 - Período 3: 37 a 61 horas (p. 191)
 - Período 4: 62 a 72 horas (p. 192)
 - Período 5: 73 a 75 horas (p. 193)
 - Período 6: 76 a 90 horas (p. 193)
 - Período 7: 91 a 96 horas (p. 194)

Conceitos do modo padrão

O modo `standard` é uma opção de configuração para instâncias expansíveis. Ele pode ser habilitado ou desabilitado a qualquer momento para uma instância interrompida ou em execução. Você pode definir `standard` como a opção de crédito padrão no nível da conta por região da AWS, por família de instâncias expansíveis, para que todas as novas instâncias de performance com capacidade de intermitência na conta sejam executadas usando a opção de crédito padrão.

Como funcionam as instâncias expansíveis padrão

Quando uma instância expansível configurada como `standard` estiver em um estado de execução, ela receberá continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos ganhos por hora. Para T2 padrão, quando a instância é interrompida, ela perde todos os créditos acumulados, e seu saldo de créditos é redefinido para zero. Quando é reiniciada, ela recebe um novo conjunto de créditos de execução e começa a acumular créditos ganhos. Para instâncias T3a e T3 padrão, o saldo de crédito de CPU persiste durante sete dias após a instância ser interrompida, e os créditos são perdidos após esse período. Se você iniciar a instância dentro de sete dias, nenhum crédito será perdido.

As instâncias padrão T2 recebem dois tipos de créditos de CPU: créditos ganhos e créditos de execução. Quando uma instância T2 padrão estiver em um estado de execução, ela recebe continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos ganhos por hora. No começo, ela ainda não ganhou créditos para uma boa experiência de inicialização. Portanto, para oferecer uma boa experiência de startup, ela recebe créditos de execução para começar, que ela gasta primeiro ao acumular créditos ganhos.

As instâncias T3a e T3 não recebem créditos de inicialização porque são compatíveis com o modo ilimitado. A configuração de crédito de modo ilimitado permite que as instâncias T4g, T3a e T3 usem o máximo de CPU necessário para expandir além da linha de base e pelo tempo necessário.

Créditos de execução

As instâncias T2 padrão recebem 30 créditos de execução por vCPU na execução ou inicialização. Por exemplo, uma instância `t2.micro` tem uma vCPU e recebe 30 créditos de execução, enquanto uma instância `t2.xlarge` tem quatro vCPUs e recebe 120 créditos de execução. Os créditos de execução foram criados para oferecer uma boa experiência de startup, permitindo, assim, que as instâncias apresentem uma intermitência imediatamente após a execução, antes que acumulem créditos ganhos.

Os créditos de execução são gastos primeiro, antes dos créditos ganhos. Os créditos de execução não são acumulados no saldo de créditos de CPU, mas não são contabilizados para o limite de saldo de créditos de CPU. Por exemplo, uma instância `t2.micro` tem um limite de saldo de créditos de CPU de 144 créditos ganhos. Se for executada e permanecer inativa por 24 horas, seu saldo de créditos de CPU atingirá 174 (30 créditos de execução + 144 créditos ganhos), que é acima do limite. No entanto,

depois que a instância gastar os 30 créditos de execução, o saldo não poderá exceder 144. Para obter mais informações sobre o limite de saldo de crédito de CPU para cada tamanho de instância, consulte a [Tabela de créditos \(p. 175\)](#).

A tabela a seguir lista a alocação de crédito de CPU inicial recebida na execução ou na inicialização, e o número de vCPUs.

Tipo de instância	Créditos de execução	vCPUs
t1.micro	15	1
t2.nano	30	1
t2.micro	30	1
t2.small	30	1
t2.medium	60	2
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

Limites de crédito de execução

Existe um limite para o número de vezes em que instâncias T2 padrão podem receber créditos de execução. O limite padrão é de 100 execuções ou inicializações de todas as instâncias T2 padrão combinadas por conta, por região, por período de 24 horas de acúmulo. Por exemplo, o limite é atingido quando uma instância é interrompida e iniciada 100 vezes em um período de 24 horas, ou quando 100 instâncias são executadas em um período de 24 horas ou outras combinações que se igualem a 100 inicializações. As novas contas podem ter um limite inferior, que aumenta ao longo do tempo com base no seu uso.

Tip

Para garantir que as workloads sempre obtenham a performance de que precisam, alterne para [Modo ilimitado de instâncias expansíveis \(p. 177\)](#) ou considere o uso de uma instância maior.

Diferenças entre créditos de execução e créditos ganhos

A tabela a seguir lista as diferenças entre créditos de execução e créditos ganhos.

	Créditos de execução	Créditos ganhos
Taxa de ganhos de crédito	As instâncias T2 padrão recebem 30 créditos de execução por vCPU na execução ou inicialização. Se uma instância T2 for alterada de unlimited para standard , ela não obtém créditos de execução no momento em que é alterada.	Cada instância T2 obtém continuamente (a uma resolução no nível de milissegundo) uma taxa definida de créditos de CPU por hora, dependendo do tamanho da instância. Para obter mais informações sobre o número de créditos de CPU ganhos por tamanho de instância, consulte a Tabela de créditos (p. 175) .
Limite de ganho de crédito	O limite para receber créditos de execução é de 100 execuções ou inicializações de todas as instâncias T2	Uma instância T2 não pode acumular mais créditos do que o limite de saldo de crédito de CPU. Se o saldo de créditos

	Créditos de execução	Créditos ganhos
	padrão combinadas por conta, por região, por período de 24 horas de acúmulo. As novas contas podem ter um limite inferior, que aumenta ao longo do tempo com base no seu uso.	de CPU atingir o limite, todos os créditos que forem obtidos após o limite ser atingido serão descartados. Os créditos de execução não contam para o limite. Para obter mais informações sobre o limite de saldo de créditos de CPU para cada tamanho de instância T2, consulte a Tabela de créditos (p. 175) .
Uso de crédito	Os créditos de execução são gastos primeiro, antes dos créditos ganhos.	Os créditos ganhos são gastos só após todos os créditos de execução serem gastos.
Expiração de crédito	Quando uma instância T2 está em execução, os créditos de execução não expiram. Quando uma instância padrão T2 para ou é alterada para T2 ilimitada, todos os créditos de execução são perdidos.	Quando uma instância T2 está em execução, os créditos ganhos que foram acumulados não expiram. Quando a instância T2 é interrompida, todos os créditos ganhos que foram acumulados são perdidos.

O número de créditos de execução e créditos ganhos acumulados é monitorado pela métrica `CPUCreditBalance` do CloudWatch. Para obter mais informações, consulte `CPUCreditBalance` na [Tabela de métricas do CloudWatch \(p. 201\)](#).

Exemplos de modo padrão

Os seguintes exemplos explicam o uso de créditos quando as instâncias estão configuradas como `standard`.

Exemplos

- [Exemplo 1: explicar o uso de créditos com T3 padrão \(p. 188\)](#)
- [Exemplo 2: explicar o uso de créditos com T2 padrão \(p. 189\)](#)

Exemplo 1: explicar o uso de créditos com T3 padrão

Neste exemplo, você verá como uma instância `t3.nano` executada como `standard` ganha, acumula e gasta créditos ganhos. Você verá como o saldo de créditos reflete os créditos ganhos que foram acumulados.

Uma instância `t3.nano` em execução ganha 144 créditos a cada 24 horas. Seu limite de saldo de créditos é de 144 créditos ganhos. Assim que o limite é atingido, os novos créditos ganhos são descartados. Para obter mais informações sobre o número de créditos que podem ser ganhos e acumulados, consulte a [Tabela de créditos \(p. 175\)](#).

Você pode iniciar uma instância T3 padrão e usá-la imediatamente. Ou, você pode iniciar uma instância padrão T3 e deixá-la inativa por alguns dias antes de executar aplicações. O fato de uma instância ser usada ou permanecer inativa determina se os créditos são acumulados ou gastos. Se uma instância permanecer inativa por 24 horas a partir do momento em que é executada, o saldo de créditos atingirá seu limite, que é o número máximo de créditos ganhos que podem ser acumulados.

Esse exemplo descreve uma instância em permanece inativa por 24 horas após sua execução e mostra sete períodos em um período de 96 horas, mostrando a taxa na qual os créditos são ganhos, acumulados, gastos e descartados, e o valor do saldo no final de cada período.

O fluxo de trabalho a seguir faz referência aos pontos numerados no gráfico:

P1 – às 0 horas no gráfico, a instância é executada como **standard** e começa a ganhar créditos imediatamente. A instância permanece inativa desde a sua execução (o uso da CPU é de 0%), e nenhum crédito é gasto. Todos os créditos não gastos são acumulados no saldo de crédito. Nas primeiras 24 horas, **CPUCreditUsage** é de 0, e o valor **CPUCreditBalance** atinge seu máximo de 144.

P2 – nas próximas 12 horas, a utilização de CPU é de 2,5%, que é abaixo da linha de base de 5%. A instância ganha mais créditos do que gasta, mas o valor **CPUCreditBalance** não pode exceder seu máximo de 144 créditos. Todos os créditos ganhos que excedem o limite são descartados.

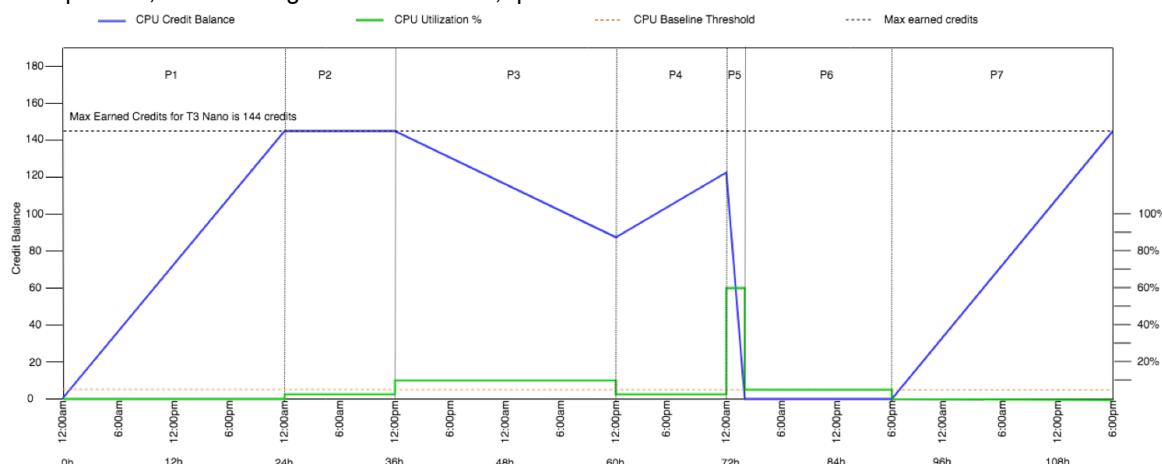
P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor **CPUCreditBalance** diminui para 86,4 créditos.

P4 – nas próximas 12 horas, a utilização de CPU diminui para 2,5% (abaixo da linha de base), o que exige um gasto de 36 créditos. Ao mesmo tempo, a instância ganha 72 créditos. A instância ganha mais créditos do que gasta, e o valor **CPUCreditBalance** aumenta para 122 créditos.

P5 – nas próximas duas horas, a instância tem intermitência para 100% de utilização de CPU e esgota todo o valor **CPUCreditBalance** de 122 créditos. Ao fim desse período, com o **CPUCreditBalance** em zero, a utilização de CPU é forçada a diminuir para o nível de utilização de linha de base de 5%. Na linha de base, a instância ganha o mesmo número de créditos que são gastos.

P6 – nas próximas 14 horas, a utilização de CPU é de 5%, (a linha de base). A instância ganha o mesmo número de créditos que são gastos. O valor de **CPUCreditBalance** permanece em 0.

P7 – nas últimas 24 horas neste exemplo, a instância está inativa, e a utilização de CPU é de 0%. Durante esse período, a instância ganha 144 créditos, que acumula em seu **CPUCreditBalance**.



Exemplo 2: explicar o uso de créditos com T2 padrão

Neste exemplo, você verá como uma instância **t2.nano** executada como **standard** ganha, acumula e gasta créditos ganhos e de execução. Você verá como o saldo de crédito reflete não somente os créditos ganhos acumulados, como também os créditos de execução acumulados.

A instância **t2.nano** obtém 30 créditos de execução quando é executada e ganha 72 créditos a cada 24 horas. Seu limite de saldo é de 72 créditos ganhados. Os créditos de execução não são considerados no limite. Assim que o limite é atingido, os novos créditos ganhos são descartados. Para obter mais informações sobre o número de créditos que podem ser ganhos e acumulados, consulte a [Tabela de créditos \(p. 175\)](#). Para obter mais informações sobre limites, consulte [Limites de crédito de execução \(p. 187\)](#).

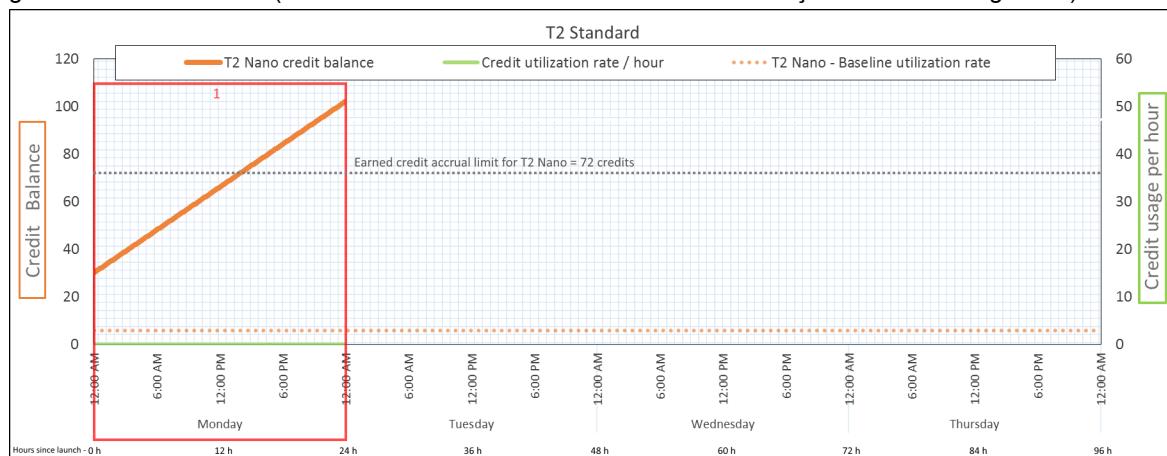
Você pode iniciar uma instância T2 padrão e usá-la imediatamente. Ou, você pode iniciar uma instância padrão T2 e deixá-la inativa por alguns dias antes de executar aplicações. O fato de uma instância ser

usada ou permanecer inativa determina se os créditos são acumulados ou gastos. Se uma instância permanecer inativa por 24 horas após sua execução, o saldo de crédito será exibido como ultrapassado do limite, pois reflete os créditos ganhos e de execução acumulados. No entanto, após o uso da CPU, os créditos de execução são gastos primeiro. Depois disso, o limite sempre reflete o número máximo de créditos ganhos que podem ser acumulados.

Esse exemplo descreve uma instância em permanece inativa por 24 horas após sua execução e mostra sete períodos em um período de 96 horas, mostrando a taxa na qual os créditos são ganhos, acumulados, gastos e descartados, e o valor do saldo no final de cada período.

Período 1: 1 a 24 horas

Na hora 0 do gráfico, a instância T2 é executada como standard e obtém imediatamente 30 créditos de execução. Ela ganha créditos durante o estado de execução. A instância permanece inativa desde a sua execução (o uso da CPU é de 0%), e nenhum crédito é gasto. Todos os créditos não gastos são acumulados no saldo de crédito. Aproximadamente 14 horas após a execução, o saldo de crédito é 72 (30 créditos de execução + 42 créditos ganhos), que é equivalente ao que a instância pode ganhar em 24 horas. Após 24 horas da execução, o saldo ultrapassa 72 créditos, pois os créditos de execução não gastos são acumulados (o saldo é de 102 créditos: 30 créditos de execução + 72 créditos ganhos).



Taxa de gasto de crédito	0 crédito por 24 horas (0% de uso da CPU)
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	0 crédito por 24 horas
Saldo de crédito	102 créditos (30 créditos de execução + 72 créditos ganhos)

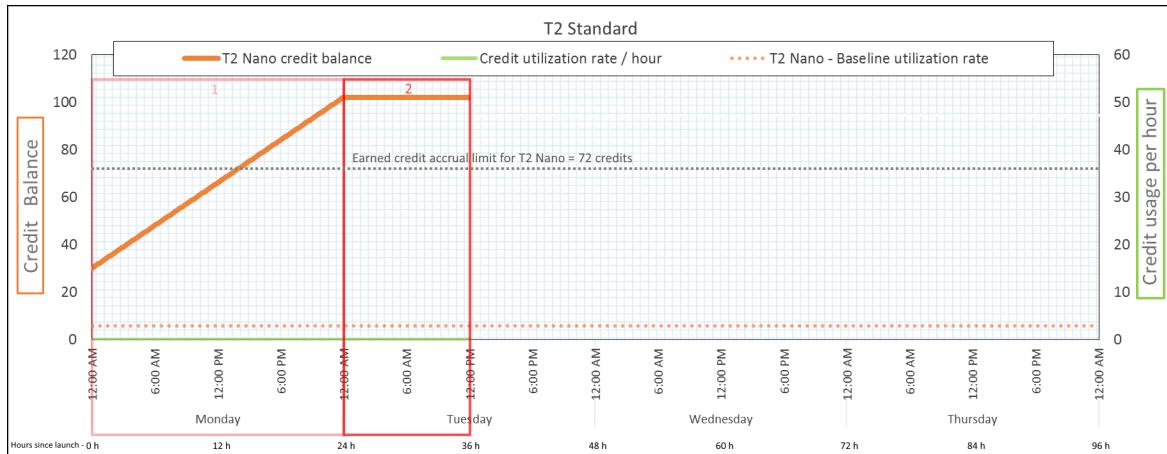
Conclusion

Se não houver uso da CPU após a execução, a instância acumulará mais créditos do que pode ganhar em 24 horas (30 créditos de execução + 72 créditos ganhos = 102).

Em um cenário real, uma instância do EC2 consome um pequeno número de créditos durante a execução. Isso impede que o saldo atinja o valor teórico máximo nesse exemplo.

Período 2: 25 a 36 horas

Nas próximas 12 horas, a instância continua ociosa e ganhando créditos, mas o saldo não aumenta. Ele estabiliza em 102 créditos (30 créditos de execução + 72 créditos ganhos). O saldo atingiu o limite de 72 créditos ganhos acumulados. Por isso, os créditos ganhos mais recentemente são descartados.



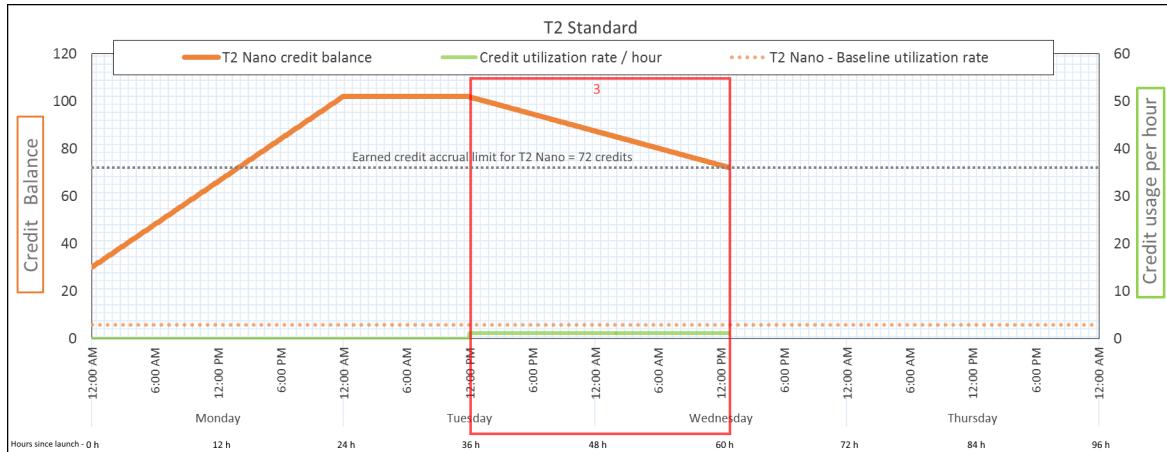
Taxa de gasto de crédito	0 crédito por 24 horas (0% de uso da CPU)
Taxa de ganhos de crédito	72 créditos por 24 horas (3 créditos por hora)
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	102 créditos (30 créditos de execução + 72 créditos ganhos) – o saldo não é alterado

Conclusion

Uma instância ganha constantemente créditos, mas, se atingir o limite, não poderá acumular mais créditos. Assim que o limite é atingido, os créditos ganhos mais recentemente são descartados. Os créditos de execução não são contabilizados para o limite de saldo de créditos de execução. Se incluir créditos de execução acumulados, o saldo parecerá estar acima do limite.

Período 3: 37 a 61 horas

Nas próximas 25 horas, a instância usa 2% da CPU. Isso requer 30 créditos. No mesmo período, ela ganha 75 créditos, mas o saldo diminui. O saldo diminui porque os créditos de execução acumulados são gastos primeiro, enquanto os créditos recém-ganhos são descartados, pois o saldo já está no limite de 72 créditos ganhos.



Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 30 créditos— em 25 horas
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (30 créditos de execução foram gastados; 72 créditos ganhos continuam não gastos)

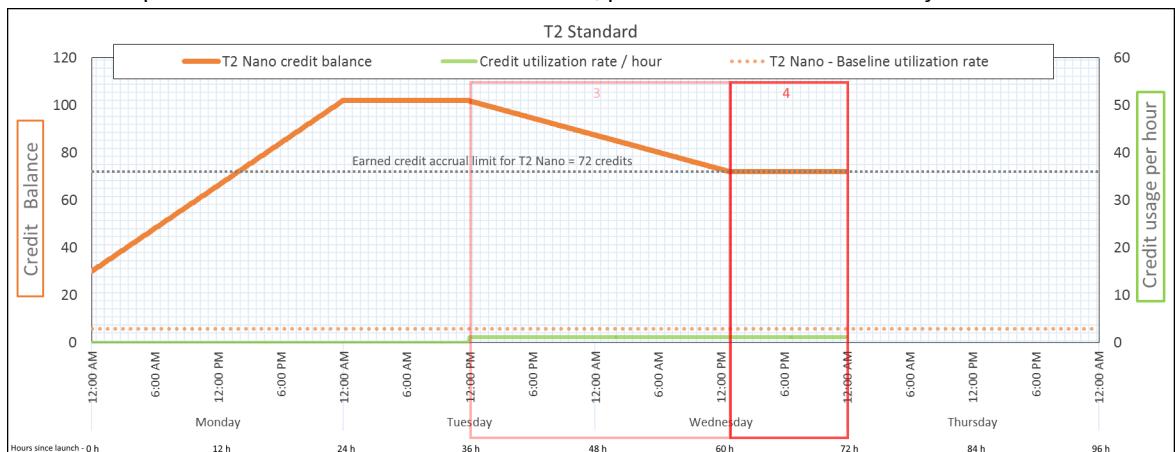
Conclusion

A instância gasta créditos de execução primeiro, antes dos crédito ganhos. Os créditos de execução não são contabilizados para o limite de créditos. Após o gasto dos créditos de execução, o saldo nunca pode ultrapassar o número ganho em 24 horas. Além disso, durante sua execução, a instância não pode obter mais créditos de execução.

Período 4: 62 a 72 horas

Nas próximas 11 horas, a instância usa 2% da CPU. Isso requer 13,2 créditos. Esse é o mesmo uso de CPU que o do período anterior, mas o saldo não diminui. Ele permanece em 72 créditos.

O saldo não diminui pois a taxa de ganho é superior à taxa de gasto de crédito. No período em que gasta 13,2 créditos, a instância também ganha 33. No entanto, o limite de saldo é de 72 créditos. Portanto, todos os créditos ganhos que ultrapassam o limite são descartados. O saldo é estabilizado em 72 créditos, que é diferente do platô de 102 créditos durante o Período 2, pois não há crédito de execução acumulado.



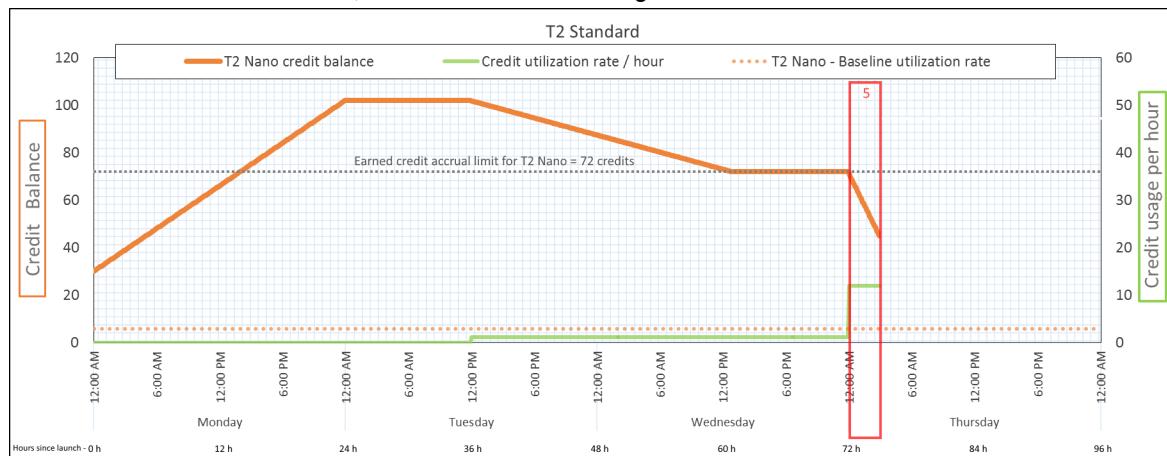
Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 13,2 —créditos em 11 horas
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	43,2 créditos por 24 horas (60% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (0 créditos de execução, 72 créditos ganhos) —saldo está no limite

Conclusion

Após o gasto dos créditos de execução, o limite de saldo de crédito é determinado pelo número de créditos que uma instância pode ganhar em 24 horas. Se a instância ganhar mais créditos do que gastar, os créditos recém-ganhos acima do limite serão descartados.

Período 5: 73 a– 75 horas

Nas próximas três horas, o uso da CPU pela instância sobe para 20%. Isso requer 36 créditos. A instância ganha nove créditos nas mesmas três horas, resultando em uma diminuição do saldo líquido de 27 créditos. No final das três horas, o saldo é de 45 créditos ganhos.



Taxa de gasto de crédito	288 créditos por 24 horas (12 créditos por hora, 20% de utilização da CPU, 400% de taxa de ganhos de crédito) – 36— créditos em 3 horas
Taxa de ganhos de crédito	72 créditos por 24 horas (9 créditos em 3 horas)
Taxa de descarte de crédito	0 crédito por 24 horas
Saldo de crédito	45 créditos (saldo anterior (72) - créditos gastos (36) + créditos ganhos (9)) – o — saldo diminui a uma taxa de 216 créditos por 24 horas (taxa de gastos de 288/24 + taxa de ganhos de 72/24 = taxa de diminuição do saldo de 216/24)

Conclusion

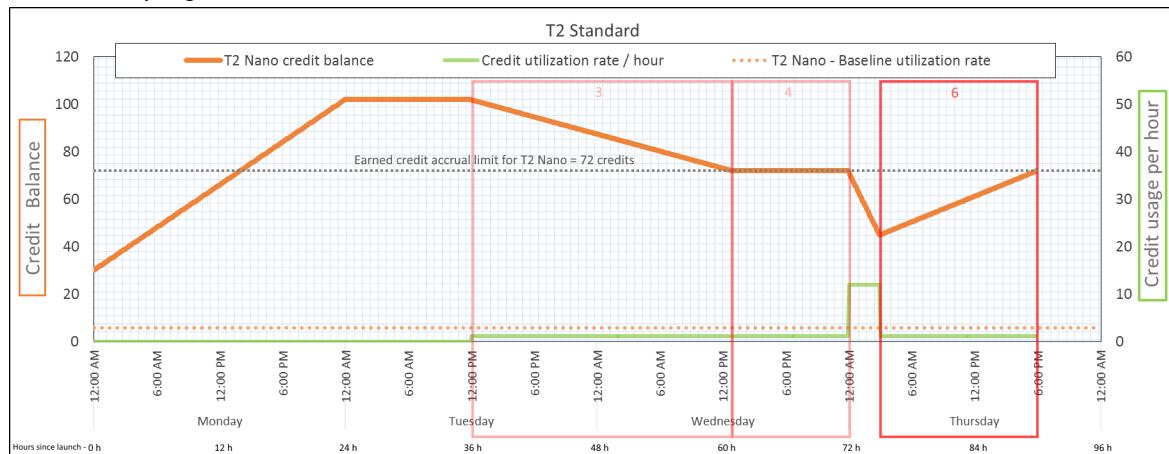
Se uma instância gastar mais créditos do que ganhar, seu balanço diminuirá.

Período 6: 76 a 90 horas

Nas próximas 15 horas, a instância usa 2% da CPU. Isso requer 18 créditos. Esta é a mesma utilização da CPU que nos períodos 3 e 4. No entanto, o saldo aumenta nesse período, embora tenha diminuído no Período 3 e estabilizado no Período 4.

No Período 3, os créditos de execução acumulados foram gastos. Todos os créditos ganhos que ultrapassaram o limite foram descartados, resultando em uma diminuição do saldo de crédito. No Período 4, a instância gastou menos créditos do que ganhou. Todos os créditos ganhos que ultrapassaram o limite foram descartados. Portanto, o saldo se estabilizou no máximo de 72 créditos.

Nesse período, não há créditos de execução acumulados, e o número de créditos ganhos acumulados no saldo está abaixo do limite. Nenhum crédito ganho é descartado. Além disso, a instância ganha mais créditos do que gasta, resultando em um aumento do saldo de crédito.



Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 18—créditos em 15 horas
Taxa de ganhos de crédito	72 créditos por 24 horas (45 créditos em 15 horas)
Taxa de descarte de crédito	0 crédito por 24 horas
Saldo de crédito	72 créditos (o saldo aumenta a uma taxa de 43,2 créditos por 24 horas – taxa de alterações = taxa de gastos de 28,8/24 + taxa de ganhos de 72/24)

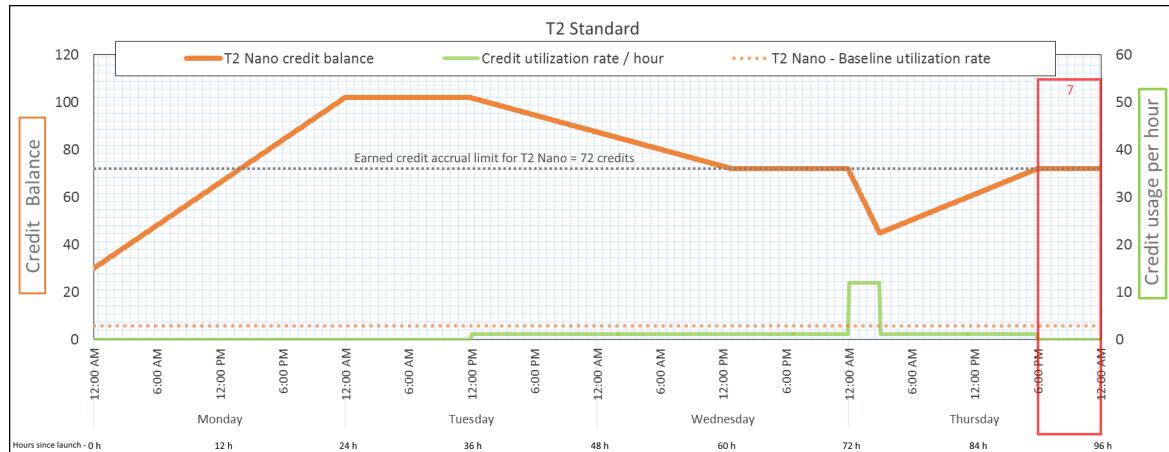
Conclusion

Se uma instância gastar menos créditos do que ganhar, seu saldo aumentará.

Período 7: 91 a 96 horas

Nas próximas seis horas, a instância permanecerá inativa —a utilização da CPU será de 0%— e nenhum crédito será gasto. Esse é o mesmo uso da CPU que no Período 2, mas o saldo não é estabilizado em 102 créditos. Ele se estabiliza em 72 créditos, —que é o limite para a instância.

No Período 2, o saldo incluiu 30 créditos de execução acumulados. OS créditos de execução foram gastos no Período 3. Uma instância em execução não pode obter mais créditos de execução. Quando o limite de saldo é atingido, os créditos ganhos ultrapassados são descartados.



Taxa de gasto de crédito	0 crédito por 24 horas (0% de uso da CPU)
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (0 créditos de execução, 72 créditos ganhos)

Conclusion

Uma instância ganha constantemente créditos, mas, se atingir o limite, não poderá acumular mais créditos. Assim que o limite é atingido, os créditos ganhos mais recentemente são descartados. O limite de saldo de crédito é determinado pelo número de créditos que uma instância pode ganhar em 24 horas. Para obter mais informações sobre os limites de saldo de crédito, consulte a [Tabela de créditos \(p. 175\)](#).

Trabalhar com instâncias expansíveis

As etapas de execução, monitoramento e modificação dessas instâncias são semelhantes. A principal diferença é a especificação de crédito padrão na execução. Se você não alterar a especificação de crédito padrão, o padrão será:

- As instâncias T3a e T3 são executadas como **unlimited**
- Instâncias T3 em um Host Dedicado são iniciadas como **standard**
- As instâncias T2 são executadas como **standard**

Tópicos

- [Iniciar uma instância expansível como ilimitada ou padrão \(p. 196\)](#)
- [Usar um grupo de Auto Scaling para executar uma instância expansível como ilimitada \(p. 196\)](#)
- [Exibir a especificação de crédito de uma instância expansível \(p. 198\)](#)
- [Modificar a especificação de crédito de uma instância expansível \(p. 199\)](#)
- [Definir a especificação de crédito padrão para a conta \(p. 200\)](#)
- [Visualizar a especificação de crédito padrão \(p. 200\)](#)

Iniciar uma instância expansível como ilimitada ou padrão

Você pode executar suas instâncias como `unlimited` ou `standard` usando o console do Amazon EC2, um AWS SDK, uma ferramenta de linha de comando ou um grupo do Auto Scaling. Para obter mais informações, consulte [Usar um grupo de Auto Scaling para executar uma instância expansível como ilimitada \(p. 196\)](#).

Para executar uma instância expansível como ilimitada ou padrão (console)

1. Siga o procedimento do [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).
2. Na página Choose an Instance Type (Escolher um tipo de instância), selecione um tipo de instância e escolha Next: Configure Instance Details (Próximo: configurar os detalhes da instância).
3. Escolha uma opção de crédito.
 - a. Para iniciar uma instância T3a e T3 como `standard`, desmarque Unlimited (Ilimitado).
 - b. Para iniciar uma instância T2 como `unlimited`, selecione Unlimited (Ilimitado).
4. Continue como solicitado pelo assistente. Ao terminar de revisar suas opções na página Review Instance Launch (Revisar execução da instância), selecione Launch (Executar). Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).

Para iniciar uma instância expansível como ilimitada ou padrão (AWS CLI)

Use o comando `run-instances` para executar suas instâncias. Especifique a opção de crédito usando o parâmetro `--credit-specification CpuCredits=`. As opções de crédito válidas são `unlimited` e `standard`.

- Para T3a e T3, se você não incluir o parâmetro `--credit-specification`, a instância será executada como `unlimited` por padrão.
- Para T2, se você não incluir o parâmetro `--credit-specification`, a instância será executada como `standard` por padrão.

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t3.micro --key-name MyKeyPair --credit-specification "CpuCredits=unlimited"
```

Usar um grupo de Auto Scaling para executar uma instância expansível como ilimitada

Quando as instâncias expansíveis são executadas ou iniciadas, elas exigem créditos de CPU para uma boa experiência de bootstrapping. Se você usar um grupo do Auto Scaling para executar suas instâncias, recomendamos configurar suas instâncias como `unlimited`. Caso faça isso, as instâncias usam créditos excedentes quando são automaticamente iniciadas ou reiniciadas pelo grupo do Auto Scaling. O uso de créditos excedentes impede restrições de performance.

Criar um modelo de execução

Você deve usar um modelo de execução para executar instâncias como `unlimited` em um grupo do Auto Scaling. Uma configuração de execução não oferece suporte à execução de instâncias como `unlimited`.

Note

O modo `unlimited` não é compatível com instâncias T3 que são iniciadas em um Host Dedicado.

Para criar um modelo de execução que execute instâncias como ilimitadas (console)

1. Siga o procedimento [Criando um modelo de execução para um grupo do Auto Scaling](#).

2. Em Launch template contents (Conteúdo do modelo de execução), para Instance type (Tipo de instância), escolha um tamanho de instância.
3. Para iniciar instâncias como `unlimited` em um grupo do Auto Scaling, em Advanced details (Detalhes avançados), para Credit specification (Especificação de crédito), escolha Unlimited (Ilimitado).
4. Ao terminar de definir os parâmetros do modelo de execução, escolha Create launch template (Criar modelo de execução). Para obter mais informações, consulte [Criar um modelo de execução para um grupo de Auto Scaling](#) no Guia do usuário do Amazon EC2 Auto Scaling.

Para criar um modelo de execução que execute instâncias como ilimitadas (AWS CLI)

Use o comando `create-launch-template` e especifique `unlimited` como a opção de crédito.

- Para T3a e T3, se você não incluir o valor `CreditSpecification={CpuCredits=unlimited}`, a instância será executada como `unlimited` por padrão.
- Em T2, se você não incluir o valor `CreditSpecification={CpuCredits=unlimited}`, a instância será executada como `standard` por padrão.

```
aws ec2 create-launch-template --launch-template-name MyLaunchTemplate
--version-description FirstVersion --launch-template-data
ImageId=ami-8c1be5f6,InstanceType=t3.medium,CreditSpecification={CpuCredits=unlimited}
```

[Associar um grupo de Auto Scaling a um modelo de execução](#)

Para associar o modelo de execução a um grupo do Auto Scaling, crie o grupo do Auto Scaling usando o modelo de execução ou adicione o modelo de execução a um grupo do Auto Scaling existente.

Para criar um grupo do Auto Scaling usando um modelo de execução (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação na parte superior da tela, selecione a mesma região usada ao criar o modelo de execução.
3. No painel de navegação, escolha Auto Scaling Groups, Criar grupo do Auto Scaling.
4. Escolha Launch Template (Modelo de execução), selecione seu modelo de execução e, seguida, Next Step (Próxima etapa).
5. Preencha os campos para o grupo do Auto Scaling. Quando você terminar de revisar as definições de configuração na Review page (Página de revisão), selecione Create Auto Scaling group (Criar grupo do Auto Scaling). Para obter mais informações, consulte [Criação de um grupo do Auto Scaling usando um modelo de execução](#) no Guia do usuário do Amazon EC2 Auto Scaling.

Para criar um grupo do Auto Scaling usando um modelo de execução (AWS CLI)

Use o comando `create-auto-scaling-group` da AWS CLI e especifique o parâmetro `--launch-template`.

Para adicionar um modelo de execução a um grupo do Auto Scaling (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação na parte superior da tela, selecione a mesma região usada ao criar o modelo de execução.
3. No painel de navegação, escolha Groups Auto Scaling.
4. Na lista de grupos do Auto Scaling, selecione um grupo do Auto Scaling, Actions (Ações) e Edit (Editar).

5. Na guia Details (Detalhes), em Launch Template (Modelo de execução), selecione um modelo de execução e, em seguida, selecione Save (Salvar).

Para adicionar um modelo de execução a um grupo do Auto Scaling (AWS CLI)

Use o comando [update-auto-scaling-group](#) da AWS CLI e especifique o parâmetro --launch-template.

Exibir a especificação de crédito de uma instância expansível

Você pode exibir a especificação de crédito (unlimited ou standard) de uma instância em execução ou interrompida.

New console

Como visualizar a especificação de crédito para uma instância com capacidade de intermitência

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância.
4. Escolha Details (Detalhes) e exiba o campo Credit specification (Especificação de crédito). O valor é unlimited ou standard.

Old console

Como visualizar a especificação de crédito para uma instância com capacidade de intermitência

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância.
4. Selecione Description (Descrição) e visualize o campo T2/T3 Unlimited (T2/T3 ilimitada).
 - Se o valor é Enabled, sua instância está configurada como unlimited.
 - Se o valor é Disabled, sua instância está configurada como standard.

Para descrever a especificação de crédito de uma instância expansível (AWS CLI)

Use o comando [describe-instance-credit-specifications](#). Se você não especificar um ou mais IDs de instâncias, todas as instâncias com a especificação de crédito unlimited serão retornadas, bem como as instâncias que foram previamente configuradas com a especificação de crédito unlimited. Por exemplo, se você redimensionar uma instância T3 para uma instância M4, enquanto a mesma estiver configurada como unlimited, o Amazon EC2 retornará a instância M4.

Example

```
aws ec2 describe-instance-credit-specifications --instance-id i-1234567890abcdef0
```

A seguir está um exemplo de saída:

```
{  
    "InstanceCreditSpecifications": [  
        {  
            "InstanceId": "i-1234567890abcdef0",  
            "CpuCredits": "unlimited"  
        }  
    ]  
}
```

]
}

Modificar a especificação de crédito de uma instância expansível

Você pode alterar a especificação de crédito de uma instância interrompida ou em execução a qualquer momento entre **unlimited** e **standard**.

New console

Como modificar a especificação de crédito para instâncias expansíveis

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância. Para modificar a especificação de crédito para várias instâncias de uma vez, selecione todas as instâncias aplicáveis.
4. Escolha Actions (Ações), Instance settings (Configurações de instância), Change credit specification (Alterar especificação de crédito). Essa opção será ativada somente se você selecionou uma instância expansível.
5. Para alterar a especificação de crédito para **unlimited**, marque a caixa de seleção ao lado do ID da instância. Para alterar a especificação de crédito para **standard**, desmarque a caixa de seleção ao lado do ID da instância.

Old console

Como modificar a especificação de crédito para instâncias expansíveis

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância. Para modificar a especificação de crédito para várias instâncias de uma vez, selecione todas as instâncias aplicáveis.
4. Selecione Actions (Ações), Instance Settings (Configurações da instância), Change T2/T3 Unlimited (Alterar T2/T3 ilimitada). Essa opção será ativada somente se você selecionou uma instância expansível.
5. A especificação de crédito atual aparece entre parênteses após o ID da instância. Para alterar a opção de crédito para **unlimited**, escolha Enable (Ativar). Para alterar a opção de crédito para **standard**, escolha Disable (Desativar).

Para modificar a opção de crédito para instâncias expansíveis (AWS CLI)

Use o comando **modify-instance-credit-specification**. Especifique a instância e sua opção de crédito usando o parâmetro **--instance-credit-specification**. As opções de crédito válidas são **unlimited** e **standard**.

Example

```
aws ec2 modify-instance-credit-specification --region us-east-1 --instance-credit-specification "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

A seguir está um exemplo de saída:

```
{  
    "SuccessfulInstanceCreditSpecifications": [  
        {  
            "InstanceId": "i- 1234567890abcdef0"  
        }  
    ]  
}
```

```
    ],
    "UnsuccessfulInstanceCreditSpecifications": []
}
```

Definir a especificação de crédito padrão para a conta

É possível definir a especificação de crédito padrão por família de instâncias expansíveis no nível da conta por região da AWS.

Se você usar o assistente de execução de instância no console do EC2 para executar instâncias, o valor selecionado para a especificação de crédito substituirá a especificação de crédito padrão no nível da conta. Se você usar a AWS CLI para executar instâncias, todas as novas instâncias expansíveis na conta serão executadas usando a opção de crédito padrão. A especificação de crédito para instâncias existentes em execução ou interrompidas não é afetada.

Consideration

A especificação de crédito padrão para uma família de instâncias pode ser modificada apenas uma vez em um período contínuo de 5 minutos e até quatro vezes em um período contínuo de 24 horas.

Como definir a especificação de crédito padrão no nível da conta (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos da conta), escolha Default credit specification (Especificação de crédito padrão).
4. Escolha Gerenciar.
5. Para cada família de instâncias, escolha Unlimited (Ilimitado) ou Standard (Padrão) e, em seguida, escolha Update (Atualizar).

Como definir a especificação de crédito padrão no nível da conta (AWS CLI)

Use o comando `modify-default-credit-specification`. Especifique a região da AWS, a família de instâncias e a especificação de crédito padrão usando o parâmetro `--cpu-credits`. As especificações de crédito padrão válidas são `unlimited` e `standard`.

```
aws ec2 modify-default-credit-specification --region us-east-1 --instance-family t2 --cpu-credits unlimited
```

Visualizar a especificação de crédito padrão

É possível visualizar a especificação de crédito padrão de uma família de instâncias expansíveis no nível da conta por região da AWS.

Como visualizar a especificação de crédito padrão no nível da conta (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos da conta), escolha Default credit specification (Especificação de crédito padrão).

Como visualizar a especificação de crédito padrão no nível da conta (AWS CLI)

Use o comando `get-default-credit-specification`. Especifique a região da AWS e a família de instâncias.

```
aws ec2 get-default-credit-specification --region us-east-1 --instance-family t2
```

Monitorar seus créditos da CPU

Você pode ver o saldo de crédito de cada instância nas métricas do Amazon EC2 por instância do console do CloudWatch.

Tópicos

- [Métricas adicionais do CloudWatch para instâncias expansíveis \(p. 201\)](#)
- [Calcular o uso de crédito da CPU \(p. 202\)](#)

Métricas adicionais do CloudWatch para instâncias expansíveis

As instâncias expansíveis têm estas métricas adicionais do CloudWatch, que são atualizadas a cada cinco minutos:

- `CPUCreditUsage` – O número de créditos de CPU gastos durante o período de medição.
- `CPUCreditBalance` – o número de créditos de CPU que uma instância acumulou. Esse saldo é esgotado quando a CPU apresenta intermitências e os créditos de CPU são gastos com mais rapidez do que são ganhos.
- `CPUSurplusCreditBalance` – O número de créditos de CPU excedentes gastos para sustentar a utilização de CPU quando o valor de `CPUCreditBalance` for zero.
- `CPUSurplusCreditsCharged` – o número de créditos de CPU excedentes que ultrapassam o [número máximo de créditos de CPU \(p. 175\)](#) que podem ser ganhos em um período de 24 horas, resultando em uma cobrança adicional.

Essas duas últimas métricas aplicam-se somente a instâncias configuradas como `unlimited`.

A tabela a seguir descreve as métricas do CloudWatch para instâncias expansíveis. Para obter mais informações, consulte [Listar as métricas disponíveis do CloudWatch para as instâncias \(p. 901\)](#).

Métrica	Descrição
<code>CPUCreditUsage</code>	O número de créditos de CPU gastos pela instância por utilização de CPU. Um crédito de CPU equivale a um vCPU em execução em 100% de utilização por um minuto ou a uma combinação equivalente de vCPUs, utilização e tempo (por exemplo, um vCPU em execução a 50% de utilização por dois minutos ou dois vCPUs em execução a 25% de utilização por dois minutos). As métricas de crédito de CPU estão disponíveis a uma frequência de apenas 5 minutos. Se você especificar um período de mais cinco minutos, use a estatística <code>Sum</code> em vez da estatística <code>Average</code> . Unidades: créditos (minutos de vCPU)
<code>CPUCreditBalance</code>	O número de créditos ganhos de CPU que uma instância acumulou desde que foi executada ou iniciada. Para a T2 Padrão, o <code>CPUCreditBalance</code> também inclui o número de créditos de execução que foram acumulados. Os créditos são acumulados no saldo de créditos após terem sido ganhos e são removidos do saldo de créditos quando são gastos. O saldo de crédito tem um limite máximo, determinado pelo tamanho da instância. Depois que o limite for atingido, todos os novos créditos ganhos serão descartados. Para a T2 Padrão, os créditos de execução não são contabilizados para o limite.

Métrica	Descrição
	<p>Os créditos do <code>CPUCreditBalance</code> são disponibilizados para que a instância gaste e apresente intermitência com uma utilização de CPU acima da linha de base.</p> <p>Quando uma instância está em execução, os créditos do <code>CPUCreditBalance</code> não expiram. Quando uma instância T3a ou T3 é interrompida, o valor de <code>CPUCreditBalance</code> persiste por sete dias. Consequentemente, todos os créditos acumulados são perdidos. Quando uma instância T2 é interrompida, o valor <code>CPUCreditBalance</code> não persiste, e todos os créditos acumulados são perdidos.</p> <p>As métricas de crédito de CPU estão disponíveis a uma frequência de apenas 5 minutos.</p> <p>Unidades: créditos (minutos de vCPU)</p>
<code>CPUSurplusCreditBalance</code>	<p>O número de créditos excedentes gastos por uma instância <code>unlimited</code> quando seu valor <code>CPUCreditBalance</code> é zero.</p> <p>O valor <code>CPUSurplusCreditBalance</code> é pago pelos créditos de CPU ganhos. Se o número de créditos excedentes ultrapassar o número máximo de créditos que a instância pode ganhar em um período de 24 horas, os créditos excedentes gastos acima do limite máximo incorrerão em uma taxa adicional.</p> <p>Unidades: créditos (minutos de vCPU)</p>
<code>CPUSurplusCreditsCharged</code>	<p>O número de créditos excedentes gastos que não são pagos pelos créditos de CPU ganhos e que, portanto, incorrem em uma cobrança adicional.</p> <p>Os créditos excedentes gastos são cobrados quando uma das seguintes situações ocorre:</p> <ul style="list-style-type: none"> • Os créditos excedentes ultrapassaram o número máximo de créditos que a instância pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora. • A instância é interrompida ou encerrada. • A instância é alterada de <code>unlimited</code> para <code>standard</code>. <p>Unidades: créditos (minutos de vCPU)</p>

Calcular o uso de crédito da CPU

O uso de créditos de CPU de instâncias é calculado por meio das métricas de instância do CloudWatch descritas na tabela anterior.

O Amazon EC2 envia as métricas ao CloudWatch a cada cinco minutos. Uma referência ao valor anterior de uma métrica em qualquer momento implica o valor anterior da métrica, enviado cinco minutos atrás.

Calcular uso de créditos de CPU de instâncias padrão

- O saldo de crédito de CPU aumentará se a utilização de CPU ficar abaixo da linha de base, quando os créditos gastos forem inferiores aos créditos ganhos no intervalo anterior de cinco minutos.

- O saldo de crédito de CPU diminuirá se a utilização de CPU ficar acima da linha de base, quando os créditos gastos forem superiores aos créditos ganhos no intervalo anterior de cinco minutos.

Matematicamente, isso é capturado pela equação a seguir:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -  
CPUCreditUsage]
```

O tamanho da instância determina o número de créditos que a instância pode ganhar por hora e o número de créditos ganhos que ela pode acumular no saldo de créditos. Para obter informações sobre o número de créditos ganhos por hora e o limite de saldo de créditos para cada tamanho de instância, consulte a [Tabela de créditos \(p. 175\)](#).

Example

Este exemplo usa uma instância t3.nano. Para calcular o valor CPUCreditBalance da instância, use a equação anterior, da seguinte maneira:

- CPUCreditBalance – O saldo de crédito atual a ser calculado.
- prior CPUCreditBalance – O saldo de crédito de cinco minutos atrás. Neste exemplo, a instância acumulou dois créditos.
- Credits earned per hour – A instância t3.nano ganha seis créditos por hora.
- 5/60 – Representa o intervalo de cinco minutos entre a publicação da métrica do CloudWatch. Multiplique os créditos ganhos a cada hora por 5/60 (cinco minutos) para obter o número de créditos que a instância ganhou nos últimos cinco minutos. A instância t3.nano ganha 0,5 crédito a cada cinco minutos.
- CPUCreditUsage – Quantos créditos a instância gastou nos últimos cinco minutos. Neste exemplo, a instância gastou um crédito nos últimos cinco minutos.

Com esses valores, você pode calcular o valor CPUCreditBalance:

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Cálculo de uso de créditos de CPU de instâncias ilimitadas

Quando uma instância expansível precisa ter uma intermitência acima da linha de base, ela sempre gasta os créditos acumulados antes dos créditos excedentes. Quando ela esgotar o saldo de crédito de CPU acumulado, poderá gastar os créditos excedentes para intermitência de CPU enquanto precisar. Quando a utilização de CPU ficar abaixo da linha de base, os créditos excedentes sempre serão pagos antes que a instância acumule créditos ganhos.

Usamos o termo `Adjusted balance` nas equações a seguir para refletir a atividade que ocorre nesse intervalo de cinco minutos. Usamos esse valor para atingir os valores das métricas do CPUCreditBalance de CPUSurplusCreditBalance e CloudWatch.

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits  
earned per hour * (5/60) - CPUCreditUsage]
```

O valor 0 em `Adjusted balance` indica que a instância gastou todos os créditos ganhos para intermitência e nenhum crédito excedente foi gasto. Consequentemente, `CPUCreditBalance` e `CPUSurplusCreditBalance` são definidos como 0.

Um valor `Adjusted balance` positivo indica que a instância acumulou créditos ganhos, e os créditos excedentes anteriores (se houver) foram pagos. Consequentemente, o valor de `Adjusted balance` é atribuído a `CPUCreditBalance`, e `CPUSurplusCreditBalance` é definido como 0. O tamanho da instância determina o [número máximo de créditos \(p. 175\)](#) que ela pode acumular.

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]  
CPUSurplusCreditBalance = 0
```

O valor `Adjusted balance` negativo indica que a instância gastou todos os créditos ganhos acumulados e também os créditos excedentes gastos para intermitência. Consequentemente, o valor de `Adjusted balance` é atribuído a `CPUSurplusCreditBalance`, e `CPUCreditBalance` é definido como 0. Novamente, o tamanho da instância determina o [número máximo de créditos \(p. 175\)](#) que ela pode acumular.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]  
CPUCreditBalance = 0
```

Se os créditos excedentes gastos ultrapassarem o máximo de créditos que a instância pode acumular, o saldo de créditos excedentes será definido como o número máximo, conforme exibido na equação anterior. Os créditos excedentes restantes serão cobrados conforme representados pela métrica `CPUSurplusCreditsCharged`.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Por fim, quando a instância for encerrada, todos os créditos excedentes monitorados pelo `CPUSurplusCreditBalance` serão cobrados. Se a instância for alterada de `unlimited` para `standard`, todo o `CPUSurplusCreditBalance` restante também será cobrado.

Instâncias otimizadas para computação

Instâncias otimizadas para computação são ideais para aplicações com uso intensivo de computação que se beneficiam de processadores de alta performance.

Instâncias C5 e C5n

Essas instâncias são ideais para o seguinte:

- Workloads de processamento em lote
- Transcodificação de mídia
- Servidores Web de alta performance
- High-Performance Computing (HPC – Computação de alta performance)
- Modelagem científica
- Servidores de jogos dedicados e mecanismos de fornecimento de anúncios
- Inferência de Machine Learning e outras aplicações com uso intensivo de computação

As instâncias bare metal, como a `c5.metal`, fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória.

Para obter mais informações, consulte [Instâncias C5 do Amazon EC2](#).

Tópicos

- [Especificações de hardware \(p. 205\)](#)
- [Da performance da instância \(p. 207\)](#)
- [Performance das redes \(p. 207\)](#)
- [Performance de E/S em SSD \(p. 208\)](#)
- [Recursos da instância \(p. 209\)](#)
- [Notas de release \(p. 210\)](#)

Especificações de hardware

Este é um resumo das especificações de hardware para instâncias otimizadas para computação.

Tipo de instância	vCPUs padrão	Memória (GiB)
<code>c4.large</code>	2	3,75
<code>c4.xlarge</code>	4	7,5
<code>c4.2xlarge</code>	8	15
<code>c4.4xlarge</code>	16	30
<code>c4.8xlarge</code>	36	60
<code>c5.large</code>	2	4
<code>c5.xlarge</code>	4	8
<code>c5.2xlarge</code>	8	16
<code>c5.4xlarge</code>	16	32
<code>c5.9xlarge</code>	36	72
<code>c5.12xlarge</code>	48	96
<code>c5.18xlarge</code>	72	144
<code>c5.24xlarge</code>	96	192
<code>c5.metal</code>	96	192
<code>c5a.large</code>	2	4
<code>c5a.xlarge</code>	4	8
<code>c5a.2xlarge</code>	8	16
<code>c5a.4xlarge</code>	16	32
<code>c5a.8xlarge</code>	32	64
<code>c5a.12xlarge</code>	48	96

Tipo de instância	vCPUs padrão	Memória (GiB)
c5a.16xlarge	64	128
c5a.24xlarge	96	192
c5ad.large	2	4
c5ad.xlarge	4	8
c5ad.2xlarge	8	16
c5ad.4xlarge	16	32
c5ad.8xlarge	32	64
c5ad.12xlarge	48	96
c5ad.16xlarge	64	128
c5ad.24xlarge	96	192
c5d.large	2	4
c5d.xlarge	4	8
c5d.2xlarge	8	16
c5d.4xlarge	16	32
c5d.9xlarge	36	72
c5d.12xlarge	48	96
c5d.18xlarge	72	144
c5d.24xlarge	96	192
c5d.metal	96	192
c5n.large	2	5.25
c5n.xlarge	4	10.5
c5n.2xlarge	8	21
c5n.4xlarge	16	42
c5n.9xlarge	36	96
c5n.18xlarge	72	192
c5n.metal	72	192

Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte [Amazon EC2 Instance Types](#) (Tipos de instância do Amazon EC2).

Para obter mais informações sobre como especificar opções de CPU, consulte [Otimizar as opções de CPU \(p. 582\)](#).

Da performance da instância

As instâncias otimizadas para EBS permitem que você tenha uma performance consistentemente alta para seus volumes do EBS ao eliminar a contenção entre E/S do Amazon EBS e outros tráfegos de rede da sua instância. Algumas instâncias otimizadas para computação são otimizadas para EBS por padrão, sem nenhum custo adicional. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

Performance das redes

É possível habilitar a rede avançada em tipos de instâncias compatíveis para fornecer latências mais baixas, jitter de rede mais baixo e melhor performance de pacotes por segundo (PPS). A maioria das aplicações não precisa de um alto nível de performance de rede constantemente, mas pode se beneficiar com uma largura de banda maior ao enviar ou receber dados. Para obter mais informações, consulte [Rede avançada no Windows \(p. 1028\)](#).

Este é um resumo da performance de rede para instâncias otimizadas para computação que oferecem suporte às redes aprimoradas.

Tipo de instância	Performance das redes	Redes avançadas
c4.large	Moderada	Intel 82599 VF (p. 1037)
c4.xlarge c4.2xlarge c4.4xlarge	Alto	Intel 82599 VF (p. 1037)
c5.4xlarge e menor c5a.4xlarge e menor c5ad.4xlarge e menor c5d.4xlarge e menor	Até 10 Gbps †	ENA (p. 1029)
c4.8xlarge	10 Gbps	Intel 82599 VF (p. 1037)
c5.9xlarge c5a.8xlarge c5ad.8xlarge c5d.9xlarge	10 Gbps	ENA (p. 1029)
c5.12xlarge c5a.12xlarge c5ad.12xlarge c5d.12xlarge	12 Gbps	ENA (p. 1029)
c5n.4xlarge e menor	Até 25 Gbps †	ENA (p. 1029)
c5.18xlarge c5.24xlarge c5.metal c5d.18xlarge c5d.24xlarge c5d.metal	25 Gbps	ENA (p. 1029)
c5n.9xlarge	50 Gbps	ENA (p. 1029)
c5n.18xlarge c5n.metal	100 Gbps	ENA (p. 1029)

† Estas instâncias têm uma largura de banda de linha de base e podem usar um mecanismo de crédito de E/S de rede para ultrapassar sua largura de banda de linha de base conforme o melhor esforço. Para obter mais informações, consulte a [largura de banda da rede \(p. 1026\)](#).

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
c5.large	.75	10

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
c5.xlarge	1.25	10
c5.2xlarge	2,5	10
c5.4xlarge	5	10
c5a.large	.75	10
c5a.xlarge	1.25	10
c5a.2xlarge	2,5	10
c5a.4xlarge	5	10
c5ad.large	.75	10
c5ad.xlarge	1.25	10
c5ad.2xlarge	2,5	10
c5ad.4xlarge	5	10
c5d.large	.75	10
c5d.xlarge	1.25	10
c5d.2xlarge	2,5	10
c5d.4xlarge	5	10
c5n.large	3	25
c5n.xlarge	5	25
c5n.2xlarge	10	25
c5n.4xlarge	15	25

Performance de E/S em SSD

Se você utilizar todos os volumes de armazenamento de instâncias baseados em SSD disponíveis para sua instância, você obterá a performance de IOPS (tamanho de bloco de 4.096 bytes) na tabela a seguir (na saturação de profundidade de fila). Do contrário, você terá uma performance de IOPS inferior.

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
c5ad.large	16.283	7.105
c5ad.xlarge	32.566	14.211
c5ad.2xlarge	65.132	28.421
c5ad.4xlarge	130.263	56.842
c5ad.8xlarge	260.526	113.684

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
c5ad.12xlarge	412,500	180.000
c5ad.16xlarge	521.053	227.368
c5ad.24xlarge	825.000	360.000
c5d.large *	20.000	9.000
c5d.xlarge *	40.000	18.000
c5d.2xlarge *	80.000	37.000
c5d.4xlarge *	175.000	75.000
c5d.9xlarge	350.000	170.000
c5d.12xlarge	700.000	340.000
c5d.18xlarge	700.000	340.000
c5d.24xlarge	1.400.000	680.000
c5d.metal	1.400.000	680.000

* Para essas instâncias, você pode obter a performance especificada.

Ao preencher os volumes baseados de armazenamento de instâncias baseados em SSD, o número de IOPS de gravação que você pode atingir diminui. Isso se deve ao trabalho extra que o controlador SSD deve fazer para encontrar espaço disponível, regravar os dados existentes e apagar o espaço não utilizado para que possa ser regravado. Esse processo de coleta de lixo resulta em uma amplificação da gravação interna no SSD, expressa como uma proporção entre as operações de gravação SSD e as operações de gravação do usuário. Essa redução na performance será ainda maior se as operações de gravação não ocorrerem em múltiplos de 4.096 bytes ou não estiverem alinhadas com um limite de 4.096 bytes. Se você gravar uma quantidade menor de bytes ou os bytes que não estejam alinhados, o controlador SSD deverá ler os dados adjacentes e armazenar o resultado em um novo local. Esse padrão resulta em uma amplificação da gravação muito maior, maior latência e uma performance de E/S drasticamente reduzida.

Os controladores SSD podem usar várias estratégias para reduzir o impacto da amplificação da gravação. Uma dessas estratégias é reservar espaço no armazenamento de instâncias SSD para que o controlador possa gerenciar, com mais eficiência, o espaço disponível para operações de gravação. Isso é denominado superprovisionamento. Os volumes de armazenamento de instâncias baseados em SSD fornecidos a uma instância não têm espaço reservado para o superprovisionamento. Para reduzir a amplificação da gravação, recomendamos que você deixe 10% do volume não particionado de modo que o controlador SSD possa usá-lo para superprovisionamento. Isso diminui o armazenamento que você pode usar, mas aumenta a performance mesmo se o disco estiver próximo da capacidade total.

Para volumes de armazenamento de instâncias que oferecem suporte a TRIM, você pode usar o comando TRIM para notificar o controlador de SSD sempre quando você não precisa mais dos dados que gravou. Isso fornece ao controlador mais espaço livre, o que pode reduzir a amplificação da gravação e aumentar a performance. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 1504\)](#).

Recursos da instância

A seguir está um resumo dos recursos para instâncias otimizadas de computação:

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
C4	Sim	Não	Não	Sim
C5	Sim	Sim	Não	Sim
C5a	Sim	Sim	Não	Sim
C5ad	Não	Sim	NVMe *	Sim
C5d	Não	Sim	NVMe *	Sim
C5n	Sim	Sim	Não	Sim

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

Para obter mais informações, consulte:

- [Amazon EBS e NVMe em instâncias Windows \(p. 1438\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#)
- [Grupos de posicionamento \(p. 1044\)](#)

Notas de release

- As instâncias C5 e C5d têm um processador da série Intel Xeon Platinum 8000 de 3,1 GHz da primeira geração (Skylake-SP) ou da segunda geração (Cascade Lake).
- As instâncias C5a e C5ad apresentam um processador AMD EPYC (Rome) de segunda geração que funciona em frequências tão altas quanto 3,3. GHz.
- As instâncias C4 e instâncias baseadas no [sistema Nitro \(p. 154\)](#) exigem AMIs de HVM com suporte para EBS de 64 bits. Elas têm mais memória e exigem um sistema operacional de 64 bits para beneficiar-se dessa capacidade. As AMIs HVM fornecem performance superior em comparação com uso de AMIs paravirtuais (PV) em tipos de instância com mais memória. Além disso, você deve usar a AMI HVM para aproveitar a rede maior.
- As instâncias criadas no Sistema Nitro têm os seguintes requisitos:
 - Os [drivers de NVMe \(p. 1438\)](#) devem estar instalados
 - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1029\)](#) devem estar instalados

As [AMIs do Windows da AWS \(p. 29\)](#) atuais atendem a esses requisitos.

- As instâncias criadas nas instâncias do Sistema Nitro oferecem suporte a um máximo de 28 anexos, incluindo interfaces de rede, volumes do EBS e volumes de armazenamento de instâncias do NVMe. Para obter mais informações, consulte [Limites de volumes do Sistema Nitro \(p. 1507\)](#).
- Executar uma instância bare metal inicializa o servidor subjacente, o que inclui a verificação de todos os componentes de hardware e firmware. Isso significa que pode levar 20 minutos a partir do momento em que a instância entra no estado de execução até que ela se torne disponível na rede.
- Para anexar ou separar volumes do EBS ou interfaces de rede secundárias de uma instância bare metal, é necessário ter suporte PCIe hotplug nativo.
- As instâncias bare metal usam um dispositivo serial baseado em PCI em vez de um dispositivo serial baseado em porta de E/S. O kernel Linux upstream e as AMIs mais recentes do Amazon Linux suportam este dispositivo. As instâncias bare metal também fornecem uma tabela ACPI SPCR para permitir que o sistema use automaticamente o dispositivo serial baseado em PCI. As AMIs do Windows mais recentes usam automaticamente o dispositivo serial baseado em PCI.

- Existe um limite sobre o número total de instâncias que você pode executar em uma região e limites adicionais sobre alguns tipos de instância. Para obter mais informações, consulte [Quantas instâncias posso executar no Amazon EC2?](#) nas perguntas frequentes do Amazon EC2.

Instâncias otimizadas para memória

As instâncias otimizadas na memória são projetadas para fornecer performance rápida para workloads que processam grandes bancos de dados na memória.

Instâncias R5, R5a, R5b e R5n

Essas instâncias são ideais para o seguinte:

- Bancos de dados relacionais de alta performance (MySQL) e NoSQL (MongoDB, Cassandra).
- Armazenamentos em cache em escala Web distribuídos que fornecem cache na memória de dados do tipo chave-valor (Memcached e Redis).
- Bancos de dados na memória que usam formatos de armazenamento físico de dados otimizados e análise para business intelligence (por exemplo, SAP HANA).
- Aplicações que executam processamento em tempo real de dados não estruturados grandes (serviços financeiros, clusters Hadoop/Spark).
- Computação de alta performance (HPC) e aplicações de Electronic Design Automation (EDA).

As instâncias R5B são compatíveis com volumes `io2` Block Express. Todos os volumes `io2` anexados a uma instância R5b durante ou após a inicialização são executados automaticamente no EBS Block Express. Para obter mais informações, consulte [Volumes io2 Block Express](#).

As instâncias bare metal, como a `r5.meta1`, fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória.

Para obter mais informações, consulte [Instâncias R5 do Amazon EC2](#).

Instâncias com alta memória (u-*)

Essas instâncias oferecem 6 TiB, 9 TiB, 12 TiB, 18 TiB e 24 TiB de memória por instância. Elas foram projetadas para executar grandes bancos de dados na memória, incluindo implantações de produção do banco de dados em memória SAP HANA.

Para obter mais informações, consulte [Instâncias com mais memória do Amazon EC2](#) e [Configuração de armazenamento para SAP HANA](#). Para obter informações sobre os sistemas operacionais compatíveis, consulte [Como migrar SAP HANA na AWS para uma instância de alta memória do EC2](#).

Instâncias X1

Essas instâncias são ideais para o seguinte:

- Bancos de dados mantidos na memória, como o SAP HANA, incluindo suporte certificado pela SAP para Business Suite S/4HANA, Business Suite on HANA (SoH), Business Warehouse on HANA (BW) e Data Mart Solutions on HANA. Para obter mais informações, consulte [SAP HANA na Nuvem AWS](#).
- Mecanismos de processamento de big data, como o Apache Spark ou Presto.
- Aplicações de computação de alta performance (HPC).

Para obter mais informações, consulte [Instâncias X1 do Amazon EC2](#).

Instâncias X1e

Essas instâncias são ideais para o seguinte:

- Banco de dados de alta performance.
- Bancos de dados mantidos na memória como o SAP HANA. Para obter mais informações, consulte [SAP HANA na Nuvem AWS](#).
- Aplicações empresariais com uso intensivo de memória.

Para obter mais informações, consulte [Instâncias X1e do Amazon EC2](#).

Instâncias z1d

Essas instâncias oferecem computação e memória elevados e são ideais para o seguinte:

- Electronic Design Automation (EDA)
- Workloads de bancos de dados relacionais

As instâncias `z1d.metal` fornecem às aplicações acesso direto aos recursos físicos do servidor host, como os processadores e a memória.

Para obter mais informações, consulte [Instâncias z1d do Amazon EC2](#).

Tópicos

- [Especificações de hardware \(p. 212\)](#)
- [Performance da memória \(p. 215\)](#)
- [Performance da instância \(p. 216\)](#)
- [Performance das redes \(p. 216\)](#)
- [Performance de E/S em SSD \(p. 218\)](#)
- [Recursos da instância \(p. 220\)](#)
- [Alta disponibilidade e confiabilidade \(X1\) \(p. 220\)](#)
- [Suporte para vCPUs \(p. 221\)](#)
- [Notas de release \(p. 221\)](#)

Especificações de hardware

Este é um resumo das especificações de hardware para instâncias otimizadas para memória.

Tipo de instância	vCPUs padrão	Memória (GiB)
<code>r4.large</code>	2	15.25
<code>r4.xlarge</code>	4	30.5
<code>r4.2xlarge</code>	8	61
<code>r4.4xlarge</code>	16	122
<code>r4.8xlarge</code>	32	244
<code>r4.16xlarge</code>	64	488
<code>r5.large</code>	2	16
<code>r5.xlarge</code>	4	32
<code>r5.2xlarge</code>	8	64

Tipo de instância	vCPUs padrão	Memória (GiB)
r5.4xlarge	16	128
r5.8xlarge	32	256
r5.12xlarge	48	384
r5.16xlarge	64	512
r5.24xlarge	96	768
r5.metal	96	768
r5a.large	2	16
r5a.xlarge	4	32
r5a.2xlarge	8	64
r5a.4xlarge	16	128
r5a.8xlarge	32	256
r5a.12xlarge	48	384
r5a.16xlarge	64	512
r5a.24xlarge	96	768
r5ad.large	2	16
r5ad.xlarge	4	32
r5ad.2xlarge	8	64
r5ad.4xlarge	16	128
r5ad.8xlarge	32	256
r5ad.12xlarge	48	384
r5ad.16xlarge	64	512
r5ad.24xlarge	96	768
r5b.large	2	16
r5b.xlarge	4	32
r5b.2xlarge	8	64
r5b.4xlarge	16	128
r5b.8xlarge	32	256
r5b.12xlarge	48	384
r5b.16xlarge	64	512
r5b.24xlarge	96	768
r5b.metal	96	768

Tipo de instância	vCPUs padrão	Memória (GiB)
r5d.large	2	16
r5d.xlarge	4	32
r5d.2xlarge	8	64
r5d.4xlarge	16	128
r5d.8xlarge	32	256
r5d.12xlarge	48	384
r5d.16xlarge	64	512
r5d.24xlarge	96	768
r5d.metal	96	768
r5dn.large	2	16
r5dn.xlarge	4	32
r5dn.2xlarge	8	64
r5dn.4xlarge	16	128
r5dn.8xlarge	32	256
r5dn.12xlarge	48	384
r5dn.16xlarge	64	512
r5dn.24xlarge	96	768
r5dn.metal	96	768
r5n.large	2	16
r5n.xlarge	4	32
r5n.2xlarge	8	64
r5n.4xlarge	16	128
r5n.8xlarge	32	256
r5n.12xlarge	48	384
r5n.16xlarge	64	512
r5n.24xlarge	96	768
r5n.metal	96	768
u-6tb1.56xlarge	224	6,144
u-6tb1.112xlarge	448	6,144
u-6tb1.metal	448 *	6,144
u-9tb1.112xlarge	448	9,216

Tipo de instância	vCPUs padrão	Memória (GiB)
u-9tb1.metal	448 *	9,216
u-12tb1.112xlarge	448	12,288
u-12tb1.metal	448 *	12,288
u-18tb1.metal	448 *	18.432
u-24tb1.metal	448 *	24.576
x1.16xlarge	64	976
x1.32xlarge	128	1,952
x1e.xlarge	4	122
x1e.2xlarge	8	244
x1e.4xlarge	16	488
x1e.8xlarge	32	976
x1e.16xlarge	64	1,952
x1e.32xlarge	128	3,904
z1d.large	2	16
z1d.xlarge	4	32
z1d.2xlarge	8	64
z1d.3xlarge	12	96
z1d.6xlarge	24	192
z1d.12xlarge	48	384
z1d.metal	48	384

* Cada processador lógico é uma hyperthread em 224 cores.

Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte [Amazon EC2 Instance Types](#) (Tipos de instância do Amazon EC2).

Para obter mais informações sobre como especificar opções de CPU, consulte [Otimizar as opções de CPU](#) (p. 582).

Performance da memória

As instâncias X1 incluem buffers de memória Intel Scalable, fornecendo 300 GiB/s de largura de banda sustentável de leitura na memória e 140 GiB/s de largura de banda sustentável de gravação na memória.

Para obter mais informações sobre como a RAM pode ser habilitada para instâncias otimizadas para memória, consulte [Especificações de hardware](#) (p. 212).

As instâncias otimizadas na memória possuem mais memória e exigem AMIs HVM de 64 bits para tirar proveito dessa capacidade. As AMIs HVM fornecem performance superior em comparação com uso de AMIs paravirtuais (PV) em instâncias otimizadas para memória..

Performance da instância

As instâncias otimizadas na memória permitem maior performance criptográfica por meio do recurso Intel AES-NI mais recente, suporte ao Intel Transactional Synchronization Extensions (TSX) para impulsionar a performance do processamento de dados transacionais de memória, e suporte às instruções do processador Advanced Vector Extensions 2 (Intel AVX2) para expandir a maioria dos comandos inteiros para até 256 bits.

Performance das redes

É possível habilitar a rede avançada em tipos de instâncias compatíveis para fornecer latências mais baixas, jitter de rede mais baixo e melhor performance de pacotes por segundo (PPS). A maioria das aplicações não precisa de um alto nível de performance de rede constantemente, mas pode se beneficiar com uma largura de banda maior ao enviar ou receber dados. Para obter mais informações, consulte [Rede avançada no Windows \(p. 1028\)](#).

Este é um resumo da performance de rede para instâncias otimizadas para memória que oferecem suporte às redes aprimoradas.

Tipo de instância	Performance das redes	Redes avançadas
r4.4xlarge e menor r5.4xlarge e menor r5a.8xlarge e menor r5ad.8xlarge e menor r5b.4xlarge e menor r5d.4xlarge e menor x1e.8xlarge e menor z1d.3xlarge e menor	Até 10 Gbps †	ENA (p. 1029)
r4.8xlarge r5.8xlarge r5.12xlarge r5a.12xlarge r5ad.12xlarge r5b.8xlarge r5b.12xlarge r5d.8xlarge r5d.12xlarge x1.16xlarge x1e.16xlarge z1d.6xlarge	10 Gbps	ENA (p. 1029)
r5a.16xlarge r5ad.16xlarge	12 Gbps	ENA (p. 1029)
r5.16xlarge r5a.24xlarge r5ad.24xlarge r5b.16xlarge r5d.16xlarge	20 Gbps	ENA (p. 1029)
r5dn.4xlarge e menor r5n.4xlarge e menor	Até 25 Gbps †	ENA (p. 1029)
r4.16xlarge r5.24xlarge r5.metal r5b.24xlarge r5b.metal r5d.24xlarge r5d.metal r5dn.8xlarge r5n.8xlarge x1.32xlarge x1e.32xlarge z1d.12xlarge z1d.metal	25 Gbps	ENA (p. 1029)
r5dn.12xlarge r5n.12xlarge	50 Gbps	ENA (p. 1029)
r5dn.16xlarge r5n.16xlarge	75 Gbps	ENA (p. 1029)
r5dn.24xlarge r5dn.metal r5n.24xlarge r5n.metal u-6tb1.56xlarge u-6tb1.112xlarge u-6tb1.metal * u-9tb1.112xlarge u-9tb1.metal * u-12tb1.112xlarge u-12tb1.metal * u-18tb1.metal u-24tb1.metal	100 Gbps	ENA (p. 1029)

* Instâncias desse tipo lançadas após 12 de março de 2020 fornecem performance de rede de 100 Gbps. Instâncias desse tipo lançadas antes de 12 de março de 2020 podem fornecer apenas uma performance de rede de 25 Gbps. Para garantir que as instâncias lançadas antes de 12 de março de 2020 tenham uma performance de rede de 100 Gbps, entre em contato com a equipe de conta para atualizar a instância sem custo adicional.

† Estas instâncias têm uma largura de banda de linha de base e podem usar um mecanismo de crédito de E/S de rede para ultrapassar sua largura de banda de linha de base conforme o melhor esforço. Para obter mais informações, consulte a [largura de banda da rede \(p. 1026\)](#).

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
r5.large	.75	10
r5.xlarge	1.25	10
r5.2xlarge	2,5	10
r5.4xlarge	5	10
r5a.large	.75	10
r5a.xlarge	1.25	10
r5a.2xlarge	2,5	10
r5a.4xlarge	5	10
r5a.8xlarge	7,5	10
r5ad.large	.75	10
r5ad.xlarge	1.25	10
r5ad.2xlarge	2,5	10
r5ad.4xlarge	5	10
r5ad.8xlarge	7,5	10
r5b.large	.75	10
r5b.xlarge	1.25	10
r5b.2xlarge	2,5	10
r5b.4xlarge	5	10
r5d.large	.75	10
r5d.xlarge	1.25	10
r5d.2xlarge	2,5	10
r5d.4xlarge	5	10
r5dn.large	2.1	25
r5dn.xlarge	4.1	25
r5dn.2xlarge	8.125	25

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
r5dn.4xlarge	16.25	25
r5n.large	2.1	25
r5n.xlarge	4.1	25
r5n.2xlarge	8.125	25
r5n.4xlarge	16.25	25
z1d.large	.75	10
z1d.xlarge	1.25	10
z1d.2xlarge	2.5	10
z1d.3xlarge	5	10

Performance de E/S em SSD

Se você utilizar todos os volumes de armazenamento de instâncias baseados em SSD disponíveis para sua instância, você obterá a performance de IOPS (tamanho de bloco de 4.096 bytes) na tabela a seguir (na saturação de profundidade de fila). Do contrário, você terá uma performance de IOPS inferior.

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
r5ad.large *	30.000	15.000
r5ad.xlarge *	59.000	29.000
r5ad.2xlarge *	117.000	57.000
r5ad.4xlarge *	234.000	114.000
r5ad.8xlarge	466.666	233.333
r5ad.12xlarge	700.000	340.000
r5ad.16xlarge	933.333	466.666
r5ad.24xlarge	1.400.000	680.000
r5d.large *	30.000	15.000
r5d.xlarge *	59.000	29.000
r5d.2xlarge *	117.000	57.000
r5d.4xlarge *	234.000	114.000
r5d.8xlarge	466.666	233.333
r5d.12xlarge	700.000	340.000
r5d.16xlarge	933.333	466.666

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
r5d.24xlarge	1,400,000	680,000
r5d.metal	1,400,000	680,000
r5dn.large *	30.000	15.000
r5dn.xlarge *	59.000	29.000
r5dn.2xlarge *	117.000	57.000
r5dn.4xlarge *	234.000	114.000
r5dn.8xlarge	466.666	233.333
r5dn.12xlarge	700.000	340.000
r5dn.16xlarge	933.333	466.666
r5dn.24xlarge	1,400,000	680,000
r5dn.metal	1,400,000	680,000
z1d.large *	30.000	15.000
z1d.xlarge *	59.000	29.000
z1d.2xlarge *	117.000	57.000
z1d.3xlarge *	175.000	75.000
z1d.6xlarge	350.000	170.000
z1d.12xlarge	700.000	340.000
z1d.metal	700.000	340.000

* Para essas instâncias, você pode obter a performance especificada.

Ao preencher os volumes baseados de armazenamento de instâncias baseados em SSD, o número de IOPS de gravação que você pode atingir diminui. Isso se deve ao trabalho extra que o controlador SSD deve fazer para encontrar espaço disponível, regravar os dados existentes e apagar o espaço não utilizado para que possa ser regravado. Esse processo de coleta de lixo resulta em uma amplificação da gravação interna no SSD, expressa como uma proporção entre as operações de gravação SSD e as operações de gravação do usuário. Essa redução na performance será ainda maior se as operações de gravação não ocorrerem em múltiplos de 4.096 bytes ou não estiverem alinhadas com um limite de 4.096 bytes. Se você gravar uma quantidade menor de bytes ou os bytes que não estejam alinhados, o controlador SSD deverá ler os dados adjacentes e armazenar o resultado em um novo local. Esse padrão resulta em uma amplificação da gravação muito maior, maior latência e uma performance de E/S drasticamente reduzida.

Os controladores SSD podem usar várias estratégias para reduzir o impacto da amplificação da gravação. Uma dessas estratégias é reservar espaço no armazenamento de instâncias SSD para que o controlador possa gerenciar, com mais eficiência, o espaço disponível para operações de gravação. Isso é denominado superprovisionamento. Os volumes de armazenamento de instâncias baseados em SSD fornecidos a uma instância não têm espaço reservado para o superprovisionamento. Para reduzir a amplificação da gravação, recomendamos que você deixe 10% do volume não particionado de modo que o controlador SSD possa usá-lo para superprovisionamento. Isso diminui o armazenamento que você pode usar, mas aumenta a performance mesmo se o disco estiver próximo da capacidade total.

Para volumes de armazenamento de instâncias que oferecem suporte a TRIM, você pode usar o comando TRIM para notificar o controlador de SSD sempre quando você não precisa mais dos dados que gravou. Isso fornece ao controlador mais espaço livre, o que pode reduzir a amplificação da gravação e aumentar a performance. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 1504\)](#).

Recursos da instância

O seguinte é um resumo dos recursos de instâncias otimizadas na memória.

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
R4	Sim	Não	Não	Sim
R5	Sim	Sim	Não	Sim
R5a	Sim	Sim	Não	Sim
R5ad	Não	Sim	NVME *	Sim
R5b	Sim*	Sim	Não	Sim
R5d	Não	Sim	NVME *	Sim
R5dn	Não	Sim	NVME *	Sim
R5n	Sim	Sim	Não	Sim
Mais memória	Sim	Sim	Não	Virtualizada: sim Bare metal: não
X1	Não	Não	SSD	Sim
X1e	Não	Não	SSD*	Sim
z1d	Não	Sim	NVME *	Sim

**Todos os volumes io2 anexados a uma instância R5b durante ou após a inicialização são executados automaticamente no EBS Block Express. Para obter mais informações, consulte [io2 Block Express Volumes](#).

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

Para obter mais informações, consulte:

- [Amazon EBS e NVMe em instâncias Windows \(p. 1438\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#)
- [Grupos de posicionamento \(p. 1044\)](#)

Alta disponibilidade e confiabilidade (X1)

As instâncias X1 oferecem suporte à correção de dados de dispositivo único (SDDC +1), que detecta e corrige erros de vários bits. A SDDC +1 usa código de verificação e correção de erros para identificar e desabilitar um único dispositivo DRAM com falha.

Além disso, você pode implementar soluções de alta disponibilidade (HA) e de recuperação de desastres (DR) para atender ao objetivo de ponto de recuperação (RPO), o objetivo de tempo de recuperação (RTO) e os requisitos de custo utilizando o [Amazon CloudFormation](#) e o [Recuperar a instância \(p. 480\)](#).

Se você executar um ambiente de produção SAP HANA, você terá a opção de usar a Replicação de sistema HANA (HSR) em instâncias X1. Para obter mais informações sobre como arquitetar soluções de HA e de DR em instâncias X1, consulte [SAP HANA na Nuvem Amazon Web Services: Implantação de referência de início rápido](#).

Supporte para vCPUs

As instâncias otimizadas na memória oferecem um número alto de vCPUs, que podem provocar problemas de execução com sistemas operacionais que têm um limite menor de vCPUs. Recomendamos enfaticamente que você use as AMIs mais recentes ao executar instâncias otimizadas na memória.

As seguintes AMIs são compatíveis com a execução de instâncias otimizadas na memória:

- Amazon Linux 2 (HVM)
- Amazon Linux AMI 2016.03 (HVM) ou posterior
- Ubuntu Server 14.04 LTS (HVM)
- Red Hat Enterprise Linux 7.1 (HVM)
- SUSE Linux Enterprise Server 12 SP1 (HVM)
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 64 bits
- Windows Server 2008 SP2 64 bits

Notas de release

- As instâncias R4 oferecem até 64 vCPUs e são acionadas por dois processadores Intel XEON personalizados para a AWS com base em E5-2686v4 que oferecem largura de banda com mais memória e caches L3 maiores para impulsionar a performance de aplicações na memória.
- As instâncias R5, R5b e R5d têm um processador da série Intel Xeon Platinum 8000 de 3,1 GHz da primeira geração (Skylake-SP) ou da segunda geração (Cascade Lake).
- As instâncias R5a e R5ad têm um processador da série AMD EPYC 7000 de 2,5 GHz.
- As instâncias com mais memória (`u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal`) são as primeiras instâncias a ter uma plataforma de oito soquetes com a última geração de processadores Intel Xeon Platinum 8176M (Skylake) que são otimizados para workloads corporativas de missão crítica. As instâncias com mais memória com 18 TB e 24 TB de memória (`u-18tb1.metal` e `u-24tb1.metal`) são as primeiras instâncias desenvolvidas em uma plataforma de 8 soquetes com os processadores de segunda geração Intel Xeon Scalable 8280L (Cascade Lake).
- As instâncias X1 e X1e oferecem até 128 vCPUs e são acionadas por quatro processadores Intel Xeon E7-8880 v3 que oferecem largura de banda com mais memória e caches L3 maiores para impulsionar a performance de aplicações na memória.
- As instâncias criadas no Sistema Nitro têm os seguintes requisitos:
 - Os [drivers de NVMe \(p. 1438\)](#) devem estar instalados
 - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1029\)](#) devem estar instalados

As [AMIs do Windows da AWS \(p. 29\)](#) atuais atendem a esses requisitos.

- As instâncias criadas nas instâncias do Sistema Nitro oferecem suporte a um máximo de 28 anexos, incluindo interfaces de rede, volumes do EBS e volumes de armazenamento de instâncias do NVMe. Para obter mais informações, consulte [Limites de volumes do Sistema Nitro \(p. 1507\)](#).
- Todos os volumes `io2` anexados a uma instância R5b durante ou após a inicialização são executados automaticamente no EBS Block Express. Para obter mais informações, consulte [Volumes `io2` Block Express](#).
- Executar uma instância bare metal inicializa o servidor subjacente, o que inclui a verificação de todos os componentes de hardware e firmware. Isso significa que pode levar 20 minutos a partir do momento em que a instância entra no estado de execução até que ela se torne disponível na rede.
- Para anexar ou separar volumes do EBS ou interfaces de rede secundárias de uma instância bare metal, é necessário ter suporte PCIe hotplug nativo.
- As instâncias bare metal usam um dispositivo serial baseado em PCI em vez de um dispositivo serial baseado em porta de E/S. O kernel Linux upstream e as AMIs mais recentes do Amazon Linux suportam este dispositivo. As instâncias bare metal também fornecem uma tabela ACPI SPCR para permitir que o sistema use automaticamente o dispositivo serial baseado em PCI. As AMIs do Windows mais recentes usam automaticamente o dispositivo serial baseado em PCI.
- Você não pode executar instâncias X1 usando uma AMI do Windows Server 2008 SP2 de 64 bits, exceto para as instâncias `x1.16xlarge`.
- Você não pode executar instâncias X1e usando uma AMI do Windows Server 2008 SP2 de 64 bits.
- Com versões anteriores da AMI do Windows Server 2008 R2 de 64 bits, você não pode executar instâncias `r4.large` e `r4.4xlarge`. Se você experimentar esse problema, atualize para a versão mais recente dessa AMI.
- Existe um limite sobre o número total de instâncias que você pode executar em uma região e limites adicionais sobre alguns tipos de instância. Para obter mais informações, consulte [Quantas instâncias posso executar no Amazon EC2?](#) nas perguntas frequentes do Amazon EC2.

Instâncias otimizadas para armazenamento

As instâncias otimizadas para armazenamento foram projetadas para workloads que exijam acesso sequencial de leitura e gravação a conjuntos de dados muito grandes no armazenamento local. Elas são otimizadas para fornecer dezenas de milhares de baixa latência, operações de E/S aleatórias por segundo (IOPS) para aplicações.

Instâncias D2

Essas instâncias são ideais para o seguinte:

- Data warehouse de processamento paralelo maciço (MPP)
- Computação distribuída de MapReduce e Hadoop
- Aplicações de processamento de dados ou log

Instâncias D3 e D3en

Essas instâncias oferecem aumento do armazenamento de instâncias e são ideais para o seguintes:

- Sistemas de arquivos distribuídos para workloads do Hadoop
- Workloads de armazenamento de arquivos, como GPFS e BeeFS
- Grandes data lakes para workloads de HPC

Instâncias H1

Essas instâncias são ideais para o seguinte:

- Workloads com muitos dados, como MapReduce e sistemas de arquivos distribuídos
- Aplicações que exigem acesso sequencial a grandes quantidades de dados em armazenamento de instâncias com vínculo direto
- Aplicações que exigem acesso com alta taxa de transferência a grandes quantidades de dados

Instâncias I3 e I3en

Essas instâncias são ideais para o seguinte:

- Sistemas de processamento de transações online (OLTP) de alta frequência
- Bancos de dados relacionais
- Bancos de dados NoSQL
- Cache para bancos de dados em memória (por exemplo, Redis)
- Aplicações de data warehousing
- Sistemas de arquivos distribuídos

As instâncias bare metal fornecem às aplicações acesso direto aos recursos físicos do servidor host, como os processadores e a memória.

Para obter mais informações, consulte [Instâncias I3 do Amazon EC2](#).

Tópicos

- [Especificações de hardware \(p. 223\)](#)
- [Da performance da instância \(p. 225\)](#)
- [Performance das redes \(p. 225\)](#)
- [Performance de E/S em SSD \(p. 226\)](#)
- [Recursos da instância \(p. 227\)](#)
- [Notas de release \(p. 228\)](#)

Especificações de hardware

O armazenamento de dados primário para instâncias D2, D3 e D3en são volumes de armazenamento de instâncias HDD. O armazenamento de dados primário para instâncias I3 e I3en são volumes de armazenamento de instâncias SSD de memória expressa não volátil (NVMe).

Os volumes de armazenamento de instâncias só são persistidos durante a vida útil da instância. Quando você interrompe, encerra ou hiberna uma instância, as aplicações e os dados em seus volumes de armazenamento de instâncias são apagados. Recomendamos que você faça backup regularmente ou replique dados importantes nos volumes de armazenamento de instâncias. Para obter mais informações, consulte [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#) e [Volumes de armazenamento de instâncias SSD \(p. 1503\)](#).

Este é um resumo das especificações de hardware para instâncias otimizadas para armazenamento.

Tipo de instância	vCPUs padrão	Memória (GiB)
d2.xlarge	4	30.5
d2.2xlarge	8	61
d2.4xlarge	16	122
d2.8xlarge	36	244

Tipo de instância	vCPUs padrão	Memória (GiB)
d3.xlarge	4	32
d3.2xlarge	8	64
d3.4xlarge	16	128
d3.8xlarge	32	256
d3en.large	2	8
d3en.xlarge	4	16
d3en.2xlarge	8	32
d3en.4xlarge	16	64
d3en.6xlarge	24	96
d3en.8xlarge	32	128
d3en.12xlarge	48	192
h1.2xlarge	8	32
h1.4xlarge	16	64
h1.8xlarge	32	128
h1.16xlarge	64	256
i3.large	2	15.25
i3.xlarge	4	30.5
i3.2xlarge	8	61
i3.4xlarge	16	122
i3.8xlarge	32	244
i3.16xlarge	64	488
i3.metal	72	512
i3en.large	2	16
i3en.xlarge	4	32
i3en.2xlarge	8	64
i3en.3xlarge	12	96
i3en.6xlarge	24	192
i3en.12xlarge	48	384
i3en.24xlarge	96	768
i3en.metal	96	768

Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte [Amazon EC2 Instance Types](#) (Tipos de instância do Amazon EC2).

Para obter mais informações sobre como especificar opções de CPU, consulte [Otimizar as opções de CPU](#) (p. 582).

Da performance da instância

Para instâncias com volumes de armazenamento de instâncias de NVMe, use o driver AWS NVMe. Para obter mais informações, consulte [AWS Drivers NVMe para instâncias do Windows](#) (p. 580).

As instâncias otimizadas para EBS permitem que você tenha uma performance consistentemente alta para seus volumes do EBS ao eliminar a contenção entre E/S do Amazon EBS e outros tráfegos de rede da sua instância. Algumas instâncias otimizadas para armazenamento são otimizadas para EBS por padrão, sem nenhum custo adicional. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS](#) (p. 1440).

Performance das redes

É possível habilitar a rede avançada em tipos de instâncias compatíveis para fornecer latências mais baixas, jitter de rede mais baixo e melhor performance de pacotes por segundo (PPS). A maioria das aplicações não precisa de um alto nível de performance de rede constantemente, mas pode se beneficiar com uma largura de banda maior ao enviar ou receber dados. Para obter mais informações, consulte [Rede avançada no Windows](#) (p. 1028).

Este é um resumo da performance de rede para instâncias otimizadas para armazenamento que oferecem suporte às redes aprimoradas.

Tipo de instância	Performance das redes	Redes avançadas
d2.xlarge	Moderada	Intel 82599 VF (p. 1037)
d2.2xlarge d2.4xlarge	Alto	Intel 82599 VF (p. 1037)
i3.4xlarge e menor	Até 10 Gbps †	ENA (p. 1029)
d2.8xlarge	10 Gbps	Intel 82599 VF (p. 1037)
i3.8xlarge h1.8xlarge	10 Gbps	ENA (p. 1029)
d3.4xlarge e menor	Até 15 Gbps †	ENA (p. 1029)
d3en.2xlarge e menor i3en.3xlarge e menor	Até 25 Gbps †	ENA (p. 1029)
d3.8xlarge d3en.4xlarge i3.16xlarge i3.metal i3en.6xlarge h1.16xlarge	25 Gbps	ENA (p. 1029)
d3en.6xlarge	40 Gbps	ENA (p. 1029)
d3.8xlarge d3en.8xlarge i3en.12xlarge	50 Gbps	ENA (p. 1029)
d3en.12xlarge	75 Gbps	ENA (p. 1029)
i3en.24xlarge i3en.metal	100 Gbps	ENA (p. 1029)

† Estas instâncias têm uma largura de banda de linha de base e podem usar um mecanismo de crédito de E/S de rede para ultrapassar sua largura de banda de linha de base conforme o melhor esforço. Para obter mais informações, consulte a [largura de banda da rede \(p. 1026\)](#).

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
d3.xlarge	3	15
d3.2xlarge	6	15
d3.4xlarge	12,5	15
d3en.large	3	25
d3en.xlarge	6	25
d3en.2xlarge	12,5	25
i3en.large	2,1	25
i3en.xlarge	4,2	25
i3en.2xlarge	8,4	25
i3en.3xlarge	12,5	25

Performance de E/S em SSD

Se você utilizar todos os volumes de armazenamento de instâncias baseados em SSD disponíveis para sua instância, você obterá a performance de IOPS (tamanho de bloco de 4.096 bytes) na tabela a seguir (na saturação de profundidade de fila). Do contrário, você terá uma performance de IOPS inferior.

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
i3.large *	100,125	35.000
i3.xlarge *	206,250	70.000
i3.2xlarge	412,500	180.000
i3.4xlarge	825.000	360.000
i3.8xlarge	1,65 milhão	720.000
i3.16xlarge	3,3 milhões	1,4 milhão
i3.metal	3,3 milhões	1,4 milhão
i3en.large *	42.500	32,500
i3en.xlarge *	85.000	65.000
i3en.2xlarge *	170.000	130.000
i3en.3xlarge	250.000	200.000
i3en.6xlarge	500.000	400.000

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
i3en.12xlarge	1 milhão	800.000
i3en.24xlarge	2 milhões	1,6 milhão
i3en.metal	2 milhões	1,6 milhão

* Para essas instâncias, você pode obter a performance especificada.

Conforme você preenche os volumes de armazenamento de instâncias baseados em SSD, a performance de E/S obtida diminui. Isso se deve ao trabalho extra que o controlador SSD deve fazer para encontrar espaço disponível, regravar os dados existentes e apagar o espaço não utilizado para que possa ser regravado. Esse processo de coleta de lixo resulta em uma amplificação da gravação interna no SSD, expressa como uma proporção entre as operações de gravação SSD e as operações de gravação do usuário. Essa redução na performance será ainda maior se as operações de gravação não ocorrerem em múltiplos de 4.096 bytes ou não estiverem alinhadas com um limite de 4.096 bytes. Se você gravar uma quantidade menor de bytes ou os bytes que não estejam alinhados, o controlador SSD deverá ler os dados adjacentes e armazenar o resultado em um novo local. Esse padrão resulta em uma amplificação da gravação muito maior, maior latência e uma performance de E/S drasticamente reduzida.

Os controladores SSD podem usar várias estratégias para reduzir o impacto da amplificação da gravação. Uma dessas estratégias é reservar espaço no armazenamento de instâncias SSD para que o controlador possa gerenciar, com mais eficiência, o espaço disponível para operações de gravação. Isso é denominado superprovisionamento. Os volumes de armazenamento de instâncias baseados em SSD fornecidos a uma instância não têm espaço reservado para o superprovisionamento. Para reduzir a amplificação da gravação, recomendamos que você deixe 10% do volume não particionado de modo que o controlador SSD possa usá-lo para superprovisionamento. Isso diminui o armazenamento que você pode usar, mas aumenta a performance mesmo se o disco estiver próximo da capacidade total.

Para volumes de armazenamento de instâncias que oferecem suporte a TRIM, você pode usar o comando TRIM para notificar o controlador de SSD sempre quando você não precisa mais dos dados que gravou. Isso fornece ao controlador mais espaço livre, o que pode reduzir a amplificação da gravação e aumentar a performance. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 1504\)](#).

Recursos da instância

Veja a seguir um resumo dos recursos para instâncias otimizadas de armazenamento:

	Somente EBS	Armazenamento de instâncias	Placement group
D2	Não	HDD	Sim
D3	Não	HDD*	Sim
D3en	Não	HDD*	Sim
H1	Não	HDD*	Sim
I3	Não	NVMe *	Sim
I3en	Não	NVMe *	Sim

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

Para obter mais informações, consulte:

- [Amazon EBS e NVMe em instâncias Windows \(p. 1438\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#)
- [Grupos de posicionamento \(p. 1044\)](#)

Notas de release

- Você deve executar instâncias otimizadas de armazenamento usando uma AMI HVM.
 - As instâncias criadas no [Sistema Nitro \(p. 154\)](#) têm os seguintes requisitos:
 - Os [drivers de NVMe \(p. 1438\)](#) devem estar instalados
 - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1029\)](#) devem estar instalados
- As [AMIs do Windows da AWS \(p. 29\)](#) atuais atendem a esses requisitos.
- Executar uma instância bare metal inicializa o servidor subjacente, o que inclui a verificação de todos os componentes de hardware e firmware. Isso significa que pode levar 20 minutos a partir do momento em que a instância entra no estado de execução até que ela se torne disponível na rede.
 - Para anexar ou separar volumes do EBS ou interfaces de rede secundárias de uma instância bare metal, é necessário ter suporte PCIe hotplug nativo.
 - As instâncias bare metal usam um dispositivo serial baseado em PCI em vez de um dispositivo serial baseado em porta de E/S. O kernel Linux upstream e as AMIs mais recentes do Amazon Linux suportam este dispositivo. As instâncias bare metal também fornecem uma tabela ACPI SPCR para permitir que o sistema use automaticamente o dispositivo serial baseado em PCI. As AMIs do Windows mais recentes usam automaticamente o dispositivo serial baseado em PCI.
 - As instâncias d3.8xlarge e d3en.12xlarge oferecem suporte a um máximo de três anexos, incluindo o volume raiz. Se você exceder o limite de anexos ao adicionar uma interface de rede ou um volume do EBS, isso causará problemas de anexo na instância.
 - Existe um limite sobre o número total de instâncias que você pode executar em uma região e limites adicionais sobre alguns tipos de instância. Para obter mais informações, consulte [Quantas instâncias posso executar no Amazon EC2?](#) nas perguntas frequentes do Amazon EC2.

Windows Instâncias computacionais aceleradas do

As instâncias de computação acelerada usam aceleradores de hardware, ou coprocessadores, para executar, com mais eficiência, algumas funções, como cálculos de número de ponto flutuante, processamento gráfico ou correspondência de padrões de dados, do que o possível em software executado em CPUs. Essas instâncias permitem mais paralelismo para obter uma taxa de transferência maior em workloads com alta quantidade de computação.

Se você precisar de alta capacidade de processamento, se beneficiará do uso das instâncias de computação acelerada que concedem acesso aos aceleradores de computação com base em hardware como Graphics Processing Units (GPUs).

Tópicos

- [Instâncias de GPU \(p. 229\)](#)
- [Especificações de hardware \(p. 230\)](#)
- [Da performance da instância \(p. 231\)](#)
- [Performance das redes \(p. 231\)](#)
- [Recursos da instância \(p. 232\)](#)
- [Notas de release \(p. 233\)](#)
- [Instalar drivers NVIDIA nas instâncias do Windows \(p. 234\)](#)

- [Instalar drivers AMD nas instâncias do Windows \(p. 240\)](#)
- [Ativar NVIDIA GRID Virtual Applications \(p. 241\)](#)
- [Para otimizar as configurações de GPU \(p. 242\)](#)

Instâncias de GPU

As instâncias baseadas em GPU concedem acesso a GPUs NVIDIA com milhares de núcleos de computação. Você pode usar essas instâncias para acelerar aplicações científicas, de engenharia e renderização utilizando as estruturas de computação paralela CUDA ou Open Computing Language (OpenCL). Você também pode usá-las para aplicações gráficas, incluindo transmissão de jogos, transmissão de aplicações 3-D e outras workloads gráficas.

Se a aplicação precisar de uma pequena quantidade de aceleração gráfica, mas for mais adequado para um tipo de instância com diferentes especificações de computação, memória ou armazenamento, use um acelerador Elastic Graphics. Para obter mais informações, consulte [Amazon Elastic Graphics \(p. 850\)](#).

Instâncias G4ad e G4dn

As instâncias G4ad usam GPUs AMD Radeon Pro V520 e processadores AMD EPYC de 2^a geração e são adequadas para aplicações gráficas como estações de trabalho gráficas remotas, transmissão de jogos e renderização que aproveitam APIs padrão do setor, como OpenGL, DirectX e Vulkan. Elas fornecem até 4 GPUs AMD Radeon Pro V520, 64 vCPUs, rede de 25 Gbps e armazenamento SSD local baseado em NVME de 2,4 TB.

As instâncias G4dn usam GPUs NVIDIA Tesla e oferecem uma plataforma de alta performance e bom custo/benefício para computação com GPU de uso geral usando as estruturas CUDA ou de machine learning junto com aplicações gráficas que usam DirectX ou OpenGL. Essas instâncias proporcionam uso de rede de alta largura de banda, recursos avançados de ponto flutuante de precisão simples e meia precisão, além de precisões INT8 e INT4. Cada GPU tem 16 GiB de memória GDDR6, tornando as instâncias G4dn adequadas para inferência de machine learning, transcodificação de vídeo e aplicações gráficas, como estações de trabalho gráficas remotas e transmissão de jogos na nuvem.

Para obter mais informações, consulte [Instâncias G4 do Amazon EC2](#).

As instâncias G4dn são compatíveis com NVIDIA GRID Virtual Workstation. Para obter mais informações, consulte as [ofertas da NVIDIA no Marketplace](#).

Instâncias G3

Essas instâncias usam GPUs NVIDIA Tesla M60 e fornecem uma plataforma de alta performance, econômica, para aplicações gráficas que utilizam DirectX ou OpenGL. As instâncias G3 também fornecem recursos do NVIDIA GRID Virtual Workstation, como suporte para quatro monitores com resoluções de até 4096 x 2160, e NVIDIA GRID Virtual Applications. As instâncias G3 são adequadas para visualizações 3D, estações de trabalho remotas de uso intenso da placa de vídeo, renderização 3D, codificação de vídeo, realidade virtual e outras workloads gráficas no lado do servidor, que exigem potência de processamento altamente paralela.

Para obter mais informações, consulte [Instâncias G3 do Amazon EC2](#).

As instâncias G3 oferecem suporte a NVIDIA GRID Virtual Workstation e NVIDIA GRID Virtual Applications. Para ativar qualquer um desses recursos, consulte [Ativar NVIDIA GRID Virtual Applications \(p. 241\)](#).

Instâncias G2

Essas instâncias usam GPUs NVIDIA GRID K520 e fornecem uma plataforma de alta performance, econômica, para aplicações gráficas que utilizam DirectX ou OpenGL. Os GPUs NVIDIA GRID também

oferecem suporte às operações de API de codificação e captura rápida NVIDIA. As aplicações de exemplo incluem serviços de criação de vídeo, visualizações 3D, aplicações de uso intenso de gráfico de transmissão e outras workloads no lado do servidor.

Instâncias P3

Essas instâncias usam GPUs NVIDIA Tesla V100 e são projetadas para computação de GPU de uso geral que usa os modelos de programação CUDA ou OpenCL ou através um framework de Machine Learning. As instâncias P3 fornecem redes de alta largura de banda, recursos avançados de ponto flutuante de meia precisão, precisão única e dupla e até 32 GiB de memória por GPU, o que as torna ideais para deep learning, dinâmica computacional fluída, finanças computacionais, análise sísmica, modelagem molecular, genômica, renderização e outras workloads de computação de GPU no lado do servidor. As GPUs Tesla V100 não dão suporte ao modo de gráficos.

Para obter mais informações, consulte [Instâncias P3 do Amazon EC2](#).

As instâncias P3 oferecem suporte a transferências par a par NVIDIA NVLink. Para obter mais informações, consulte [NVIDIA NVLink](#).

Instâncias P2

As instâncias P2 usam GPUs NVIDIA Tesla K80 e são projetadas para computação de GPU de uso geral que usa os modelos de programação CUDA ou OpenCL. As instâncias P2 fornecem redes de alta largura de banda, recursos avançados de ponto flutuante de precisão única e dupla e 12 GiB de memória por GPU, o que as torna ideais para deep learning, bancos de dados gráficos, bancos de dados de alta performance, fluidodinâmica computacional, finanças computacionais, análise sísmica, modelagem molecular, genômica, renderização e outras workloads de computação de GPU no lado do servidor.

As instâncias P2 oferecem suporte a transferências par a par NVIDIA GPUDirect. Para obter mais informações, consulte [NVIDIA GPUDirect](#).

Especificações de hardware

Este é um resumo das especificações de hardware para instâncias de computação acelerada.

Tipo de instância	vCPUs padrão	Memória (GiB)	Aceleradores
p2.xlarge	4	61	1
p2.8xlarge	32	488	8
p2.16xlarge	64	732	16
p3.2xlarge	8	61	1
p3.8xlarge	32	244	4
p3.16xlarge	64	488	8
p3dn.24xlarge	96	768	8
g2.2xlarge	8	15	1
g2.8xlarge	32	60	4
g3s.xlarge	4	30.5	1
g3.4xlarge	16	122	1

Tipo de instância	vCPUs padrão	Memória (GiB)	Aceleradores
g3.8xlarge	32	244	2
g3.16xlarge	64	488	4
g4ad.xlarge	4	16	1
g4ad.2xlarge	8	32	1
g4ad.4xlarge	16	64	1
g4ad.8xlarge	32	128	2
g4ad.16xlarge	64	256	4
g4dn.xlarge	4	16	1
g4dn.2xlarge	8	32	1
g4dn.4xlarge	16	64	1
g4dn.8xlarge	32	128	1
g4dn.12xlarge	48	192	4
g4dn.16xlarge	64	256	1
g4dn.metal	96	384	8
f1.2xlarge	8	122	1
f1.4xlarge	16	244	2
f1.16xlarge	64	976	8

Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte [Amazon EC2 Instance Types](#) (Tipos de instância do Amazon EC2).

Para obter mais informações sobre como especificar opções de CPU, consulte [Otimizar as opções de CPU \(p. 582\)](#).

Da performance da instância

As instâncias otimizadas para EBS permitem que você tenha uma performance consistentemente alta para seus volumes do EBS ao eliminar a contenção entre E/S do Amazon EBS e outros tráfegos de rede da sua instância. As instâncias de computação acelerada são otimizadas para EBS por padrão, sem nenhum custo adicional. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

Performance das redes

É possível habilitar a rede avançada em tipos de instâncias compatíveis para fornecer latências mais baixas, jitter de rede mais baixo e melhor performance de pacotes por segundo (PPS). A maioria das aplicações não precisa de um alto nível de performance de rede constantemente, mas pode se beneficiar com uma largura de banda maior ao enviar ou receber dados. Para obter mais informações, consulte [Rede avançada no Windows \(p. 1028\)](#).

Este é um resumo da performance de rede para instâncias de computação acelerada que oferecem suporte às redes aprimoradas.

Tipo de instância	Performance das redes	Redes avançadas
f1.4xlarge e inferior g3.4xlarge g3s.xlarge g4ad.4xlarge e inferior p3.2xlarge	Até 10 Gbps †	ENAs (p. 1029)
g3.8xlarge p2.8xlarge p3.8xlarge	10 Gbps	ENAs (p. 1029)
g4ad.8xlarge	15 Gbps	ENAs (p. 1029)
g4dn.4xlarge e inferior	Até 25 Gbps †	ENAs (p. 1029)
f1.16xlarge g3.16xlarge g4ad.16xlarge p2.16xlarge p3.16xlarge	25 Gbps	ENAs (p. 1029)
g4dn.8xlarge g4dn.12xlarge g4dn.16xlarge	50 Gbps	ENAs (p. 1029)
g4dn.metal p3dn.24xlarge	100 Gbps	ENAs (p. 1029)

† Estas instâncias têm uma largura de banda de linha de base e podem usar um mecanismo de crédito de E/S de rede para ultrapassar sua largura de banda de linha de base conforme o melhor esforço. Para obter mais informações, consulte a [largura de banda da rede \(p. 1026\)](#).

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
g4ad.xlarge	2	10
g4ad.2xlarge	4.167	10
g4ad.4xlarge	8.333	10
g4dn.xlarge	5	25
g4dn.2xlarge	10	25
g4dn.4xlarge	20	25

Recursos da instância

Este é um resumo de recursos para instâncias de computação acelerada.

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
F1	Não	Não	NVMe *	Sim
G2	Não	Não	SSD	Sim
G3	Sim	Não	Não	Sim

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
G4ad	Não	Sim	NVMe *	Sim
G4dn	Não	Sim	NVMe *	Sim
P2	Sim	Não	Não	Sim
P3	24xlarge: não Todos os outros tamanhos: sim	24xlarge: sim Todos os outros tamanhos: não	24xlarge: NVMe *	Sim

* O volume do dispositivo raiz deve ser um volume do Amazon EBS.

Para obter mais informações, consulte:

- [Amazon EBS e NVMe em instâncias Windows \(p. 1438\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#)
- [Grupos de posicionamento \(p. 1044\)](#)

Notas de release

- Você deve executar a instância usando uma AMI de HVM.
 - As instâncias criadas no [Sistema Nitro \(p. 154\)](#) têm os seguintes requisitos:
 - Os [drivers de NVMe \(p. 1438\)](#) devem estar instalados
 - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1029\)](#) devem estar instalados
- As [AMIs do Windows da AWS \(p. 29\)](#) atuais atendem a esses requisitos.
- As instâncias baseadas em GPU não podem acessar a GPU, a menos que os drivers NVIDIA sejam instalados. Para obter mais informações, consulte [Instalar drivers NVIDIA nas instâncias do Windows \(p. 234\)](#).
 - Executar uma instância bare metal inicializa o servidor subjacente, o que inclui a verificação de todos os componentes de hardware e firmware. Isso significa que pode levar 20 minutos a partir do momento em que a instância entra no estado de execução até que ela se torne disponível na rede.
 - Para anexar ou separar volumes do EBS ou interfaces de rede secundárias de uma instância bare metal, é necessário ter suporte PCIe hotplug nativo.
 - As instâncias bare metal usam um dispositivo serial baseado em PCI em vez de um dispositivo serial baseado em porta de E/S. O kernel Linux upstream e as AMIs mais recentes do Amazon Linux suportam este dispositivo. As instâncias bare metal também fornecem uma tabela ACPI SPCR para permitir que o sistema use automaticamente o dispositivo serial baseado em PCI. As AMIs do Windows mais recentes usam automaticamente o dispositivo serial baseado em PCI.
 - Há um limite de 100 AFIs por região.
 - Existe um limite sobre o número total de instâncias que você pode executar em uma região e limites adicionais sobre alguns tipos de instância. Para obter mais informações, consulte [Quantas instâncias posso executar no Amazon EC2?](#) nas perguntas frequentes do Amazon EC2.
 - Se você executar uma instância de várias GPUs com a AMI do Windows que foi criada em uma instância de uma GPU, o Windows não instalará automaticamente o driver NVIDIA para todas as GPUs. É necessário autorizar a instalação do driver para o novo hardware de GPU. É possível corrigir isso manualmente no gerenciador de dispositivos abrindo a categoria de dispositivos Outros (as GPUs inativas não aparecem em Exibir adaptadores). Para cada GPU inativa, abra o menu de contexto

(clicando nele com o botão direito do mouse), escolha Atualizar software do driver e a opção Atualização automática padrão.

- Ao usar o Microsoft Remote Desktop Protocol (RDP), as GPUs que usam o modelo de driver WDDM são substituídas por um driver de exibição não acelerado do Remote Desktop. Recomendamos usar uma ferramenta de acesso remoto diferente para acessar sua GPU, como o [Teradici Cloud Access Software](#), o [NICE Desktop Cloud Visualization \(DCV\)](#) ou o VNC. Você também pode usar uma das AMIs de GPU do AWS Marketplace , pois elas fornecem ferramentas de acesso remoto que oferecem suporte à aceleração 3D.

Instalar drivers NVIDIA nas instâncias do Windows

Uma instância com uma GPU NVIDIA conectada, como P3 ou G4dn, deve ter o driver NVIDIA apropriado instalado. Dependendo do tipo de instância, você pode fazer download de um driver NVIDIA público, de um driver do Amazon S3 disponível somente para clientes da AWS, ou usar uma AMI com o driver pré-instalado.

Para instalar drivers AMD em uma instância com uma GPU AMD conectada, como uma instância G4ad, consulte [Instalar drivers AMD nas instâncias do Windows \(p. 240\)](#).

Sumário

- [Tipos de drivers NVIDIA \(p. 234\)](#)
- [Drivers disponíveis por tipo de instância \(p. 235\)](#)
- [Opções de instalação \(p. 235\)](#)
 - [Opção 1: AMIs com os drivers NVIDIA instalados \(p. 236\)](#)
 - [Opção 2: Drivers NVIDIA públicos \(p. 236\)](#)
 - [Opção 3: drivers GRID \(instâncias G3 e G4dn\) \(p. 237\)](#)
 - [Opção 4: drivers para jogos NVIDIA \(instâncias G4dn\) \(p. 238\)](#)
- [Instalar uma versão adicional do CUDA \(p. 239\)](#)

Tipos de drivers NVIDIA

A seguir estão os principais tipos de drivers NVIDIA que podem ser usados com as instâncias baseadas em GPU.

Drivers Tesla

Esses drivers são destinados principalmente a workloads de computação, que usam GPUs para tarefas computacionais, como cálculos de ponto flutuante paralelizados para machine learning e transformações rápidas de Fourier para aplicações de computação de alta performance.

Drivers GRID

Esses drivers são certificados para oferecer a melhor performance para aplicações de visualização profissional que renderizam conteúdo, como modelos 3D ou vídeos de alta resolução. Você pode configurar os drivers GRID para oferecer suporte a dois modos. As estações de trabalho virtuais Quadro fornecem acesso a quatro monitores de 4K por GPU. Os GRID vApps oferecem recursos de hospedagem de aplicações RDSH.

Drivers para jogos

Esses drivers contêm otimizações para jogos e são atualizados frequentemente para oferecer melhorias de performance. Eles são compatíveis com um único monitor 4K por GPU.

Modo configurado

No Windows, os drivers Tesla são configurados para serem executados no modo Tesla Compute Cluster (TCC). O driver GRID e o driver para jogos são configurados para executar no modo Windows Display Driver Model (WDDM). No modo TCC, a placa é dedicada a workloads de computação. No modo WDDM, a placa é compatível com workloads de computação e gráficos.

Painel de controle NVIDIA

O painel de controle NVIDIA é compatível com drivers GRID e para jogos. Ele não é compatível com drivers Tesla.

APIs compatíveis com drivers Tesla

- OpenCL
- NVIDIA CUDA e bibliotecas relacionadas (por exemplo, cuDNN, TensorRT, nvJPEG e cuBLAS)
- NVENC para codificação de vídeo e NVDEC para decodificação de vídeo

APIs compatíveis para GRID e drivers de jogos

- DirectX, Direct2D, DirectX Video Acceleration, DirectX Raytracing
- OpenCL, OpenGL e Vulkan
- NVIDIA CUDA e bibliotecas relacionadas (por exemplo, cuDNN, TensorRT, nvJPEG e cuBLAS)
- NVENC para codificação de vídeo e NVDEC para decodificação de vídeo

Drivers disponíveis por tipo de instância

A tabela a seguir resume os drivers NVIDIA para cada tipo de instância de GPU.

Tipo de instância	Driver Tesla	Driver GRID	Driver para jogos
G2	Não	Sim	Não
G3	Sim	Sim	Não
G4dn	Sim	Sim	Sim
P2	Sim	Não	Não
P3	Sim	Sim †	Não

† Usando somente AMIs do Marketplace

Opções de instalação

Use uma das opções a seguir para obter os drivers NVIDIA necessários para a instância de GPU.

Opções

- [Opção 1: AMIs com os drivers NVIDIA instalados \(p. 236\)](#)
- [Opção 2: Drivers NVIDIA públicos \(p. 236\)](#)
- [Opção 3: drivers GRID \(instâncias G3 e G4dn\) \(p. 237\)](#)
- [Opção 4: drivers para jogos NVIDIA \(instâncias G4dn\) \(p. 238\)](#)

Opção 1: AMIs com os drivers NVIDIA instalados

AWSA e a NVIDIA oferecem imagens de máquina da Amazon (AMI) diferentes com drivers NVIDIA instalados.

- Ofertas do Marketplace com o driver Tesla
- Ofertas do Marketplace com o driver GRID
- Ofertas do Marketplace com o driver para jogos

Se você criar uma AMI personalizada do Windows usando uma das ofertas do AWS Marketplace , a AMI deve ser uma imagem padronizada criada usando o [Sysprep \(p. 42\)](#) para garantir que o driver GRID funcione.

Opção 2: Drivers NVIDIA públicos

As opções oferecidas pela AWS são acompanhadas da licença necessária para o driver. Você também pode instalar os drivers públicos e trazer sua própria licença. Para instalar um driver público, baixe-o do site da NVIDIA conforme descrito aqui.

Você também pode usar as opções oferecidas pela AWS em vez dos drivers públicos. Para usar um driver GRID em uma instância P3, use as AMIs do AWS Marketplace conforme descrito na [Opção 1 \(p. 236\)](#). Para usar um driver GRID em uma instância G3 ou G4dn, use as AMIs do AWS Marketplace , conforme descrito na Opção 1 ou instale os drivers NVIDIA fornecidos pela AWS conforme descrito na [Opção 3 \(p. 237\)](#).

Como fazer download de um driver NVIDIA público

Faça login na instância do Windows e faça download do driver NVIDIA de 64 bits apropriado para o tipo de instância em <http://www.nvidia.com/Download/Find.aspx>. Para Tipo de produto, Séries de produtos e Produto, use as opções na tabela a seguir.

Instância	Tipo de produto	Séries de produtos	Produto
G2	GRID	Série GRID	GRID K520
G3	Tesla	M-Class	M60
G4dn †	Tesla	Série T	T4
P2	Tesla	K-Series	K80
P3	Tesla	V-Series	V100

† As instâncias G4dn requerem a versão de driver 426.00 ou posterior.

Como instalar o driver NVIDIA no Windows

1. Abra a pasta onde você fez download do driver e execute o arquivo de instalação. Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário.
2. Desabilite o adaptador de vídeo interno usando o Gerenciador de dispositivos. Instale esses recursos do Windows: Media Foundation e Quality Windows Audio Video Experience.
3. Verifique o gerenciador de dispositivos para certificar-se de que a GPU está funcionando corretamente.
4. Para obter a melhor performance na GPU, siga as etapas de otimização em [Para otimizar as configurações de GPU \(p. 242\)](#).

Opcão 3: drivers GRID (instâncias G3 e G4dn)

Esses downloads estão disponíveis somente para clientes da AWS. Ao fazer o download, você concorda que usará o software baixado somente para desenvolver AMIs para uso com o hardware NVIDIA Tesla T4 ou NVIDIA Tesla M60. Após a instalação do software, você estará vinculado aos termos do [Contrato de licença de usuário final em nuvem do NVIDIA GRID](#).

Prerequisites

- Se você executar sua instância do Windows usando uma AMI personalizada do Windows, a AMI deverá ser uma imagem padronizada criada [usando o Sysprep \(p. 42\)](#) para garantir que o driver GRID funcione.
- Configure as credenciais padrão para o AWS Tools for Windows PowerShell em sua instância do Windows. Para obter mais informações, consulte [Getting Started with the AWS Tools for Windows PowerShell](#) (Conceitos básicos do AWS Tools for Windows PowerShell) no AWS Tools for Windows PowerShell User Guide (Manual do usuário do AWS Tools for Windows PowerShell).
- Os usuários do IAM devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess.

Como instalar o driver NVIDIA GRID na instância do Windows

1. Conecte-se à instância do Windows e abra uma janela do PowerShell.
2. Faça download dos drivers e do [Contrato de licença de usuário final do NVIDIA GRID](#) do Amazon S3 para o seu desktop usando os comandos do PowerShell a seguir.

```
$Bucket = "ec2-windows-nvidia-drivers"
$keyPrefix = "latest"
$localPath = "$home\Desktop\NVIDIA"
$objects = Get-S3Object -BucketName $Bucket -KeyPrefix $keyPrefix -Region us-east-1
foreach ($object in $objects) {
    $localFileName = $object.Key
    if ($localFileName -ne '' -and $object.Size -ne 0) {
        $localFilePath = Join-Path $localPath $localFileName
        Copy-S3Object -BucketName $Bucket -Key $object.Key -LocalFile $localFilePath -Region us-east-1
    }
}
```

Várias versões de driver NVIDIA GRID são armazenadas nesse bucket. Você pode fazer download de todas as versões disponíveis no bucket removendo a opção `-KeyPrefix $keyPrefix`.

Começando no GRID versão 11.0, você pode usar os drivers no `latest` para instâncias G3 e G4dn. Não adicionaremos versões posteriores à 11.0 ao `g4/latest`, mas manteremos a versão 11.0 e as versões anteriores específicas ao G4dn no `g4/latest`.

3. Navegue até o desktop e clique duas vezes no arquivo de instalação para executá-lo (escolha a versão do driver correspondente à versão de SO da instância). Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário. Para verificar se a GPU está funcionando corretamente, verifique o gerenciador de dispositivos.
4. (Opcional) Use o comando a seguir para desabilitar a página de licenciamento no painel de controle a fim de impedir que os usuários mudem accidentalmente o tipo de produto (a NVIDIA GRID Virtual Workstation é habilitada por padrão). Para obter mais informações, consulte [Guia do usuário de licenciamento do GRID](#).

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
```

5. (Opcional) Dependendo do seu caso de uso, você pode concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

- a. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4K, configure o protocolo de exibição de alta performance, [NICE DCV](#).
- b. O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar os aplicativos virtuais GRID para recursos de hospedagem de aplicativos RDSH, conclua as etapas de ativação do aplicativo virtual GRID em [Ativar NVIDIA GRID Virtual Applications \(p. 241\)](#).

Opção 4: drivers para jogos NVIDIA (instâncias G4dn)

Esses drivers estão disponíveis somente para clientes da AWS. Ao fazer download, você concorda em usar o software baixado somente para desenvolver AMIs para uso com o hardware NVIDIA Tesla T4. Após a instalação do software, você estará vinculado aos termos do [Contrato de licença de usuário final em nuvem do NVIDIA GRID](#).

Prerequisites

- Se você executar sua instância do Windows usando uma AMI personalizada do Windows, a AMI deverá ser uma imagem padronizada criada [usando o Sysprep \(p. 42\)](#) para garantir que o driver de jogos funcione.
- Configure as credenciais padrão para o AWS Tools for Windows PowerShell em sua instância do Windows. Para obter mais informações, consulte [Getting Started with the AWS Tools for Windows PowerShell](#) (Conceitos básicos do AWS Tools for Windows PowerShell) no AWS Tools for Windows PowerShell User Guide (Manual do usuário do AWS Tools for Windows PowerShell).
- Os usuários do IAM devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess.

Como instalar o driver para jogos NVIDIA na instância do Windows

1. Conecte-se à instância do Windows e abra uma janela do PowerShell.
2. Faça download e instale o driver para jogos usando os seguintes comandos do PowerShell.

```
$Bucket = "nvidia-gaming"
$keyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $keyPrefix -Region us-east-1
foreach ($Object in $Objects) {
    $LocalFileName = $Object.Key
    if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
        $LocalFilePath = Join-Path $LocalPath $LocalFileName
        Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -Region us-east-1
    }
}
```

Muitas versões do driver NVIDIA GRID são armazenadas neste bucket do S3. Você pode fazer download de todas as versões disponíveis no bucket removendo a opção `-KeyPrefix` `$keyPrefix`.

3. Navegue até o desktop e clique duas vezes no arquivo de instalação para executá-lo (escolha a versão do driver correspondente à versão de SO da instância). Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário. Para verificar se a GPU está funcionando corretamente, verifique o gerenciador de dispositivos.
4. Crie um valor de registro na chave `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global` com o nome `vGamingMarketplace`, o tipo DWord e o valor 2. Você pode usar a janela do prompt de comando ou uma versão de 64 bits do PowerShell da seguinte forma.

- Use o seguinte comando do PowerShell para criar esse valor de registro. Por padrão, o AWS Tools for PowerShell nas AMIs do Windows da AWS é uma versão de 32 bits e ocorre falha nesse comando. Em vez disso, use a versão de 64 bits do PowerShell incluída no sistema operacional.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

- Use o seguinte comando do registro para criar esse valor de registro. Você pode executá-lo usando a janela do prompt de comando ou uma versão de 64 bits do PowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t REG_DWORD /d 2
```

5. Use o seguinte comando para fazer download do arquivo de certificação, renomeie o arquivo *GridSwCert.txt* e mova-o para a pasta Documentos Públicos no drive do sistema. Normalmente, o caminho da pasta é C:\Usuários\Público\Documentos Públicos (Windows Explorer) ou C:\Usuários \Público\Documentos (janela do prompt de comando).

- Para a versão 461.40 ou posterior:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertWindows_2021_10_2.cert" -OutFile "$Env:PUBLIC\Documents\GridSwCert.txt"
```

- Para a versão 445.87:

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents\GridSwCert.txt"
```

- Para versões anteriores

```
Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents\GridSwCert.txt"
```

6. Reinicie a instância.

7. Verifique a licença do NVIDIA Gaming usando o comando a seguir.

```
"C:\Program Files\NVIDIA Corporation\NVSMI\nvidia-smi.exe" -q
```

A saída deve ser semelhante ao seguinte.

GRID Licensed Product	
Product Name	: GRID vGaming
License Status	: Licensed

8. (Opcional) Para ajudar a aproveitar o único monitor com resolução de até 4K, configure o protocolo de exibição de alta performance [NICE DCV](#). Se você não precisar dessa funcionalidade, não conclua esta etapa.

Instalar uma versão adicional do CUDA

Depois de instalar um driver gráfico NVIDIA em sua instância, você poderá instalar uma versão do CUDA diferente da versão fornecida com o driver gráfico. O procedimento a seguir demonstra como configurar várias versões do CUDA na instância.

Como instalar o toolkit do CUDA

1. Conecte-se à sua instância do Windows.

2. Abra o site da [NVIDIA](#) e selecione a versão do CUDA que você precisa.
3. Em Installer Type (Tipo de instalador), selecione exe (local) e escolha Download (Fazer download).
4. Usando seu navegador, execute o arquivo de instalação obtido por download. Siga as instruções para instalar o toolkit do CUDA. Talvez seja necessário reiniciar a instância.

Instalar drivers AMD nas instâncias do Windows

Uma instância com uma GPU AMD conectada, como uma instância G4ad, deve ter o driver AMD apropriado instalado. Dependendo de suas necessidades, você pode usar uma AMI com o driver pré-instalado ou baixar um driver de Amazon S3.

Para instalar drivers NVIDIA em uma instância com uma GPU NVIDIA conectada, como uma instância G4dn, consulte [Instalar drivers NVIDIA nas instâncias do Windows \(p. 234\)](#).

Sumário

- [Software AMD Radeon Pro para driver empresarial \(p. 240\)](#)
- [AMIs com o driver AMD instalado \(p. 240\)](#)
- [Download do driver AMD \(p. 240\)](#)

Software AMD Radeon Pro para driver empresarial

O driver AMD Radeon Pro Software for Enterprise foi criado para oferecer suporte a casos de uso de gráficos de nível profissional. Usando o driver, você pode configurar suas instâncias com dois monitores 4K por GPU.

APIs compatíveis

- OpenGL, OpenCL
- Vulkan
- DirectX 9 e posterior
- Framework de mídia avançada da AMD
- Transformação do Microsoft Hardware Media Foundation

AMIs com o driver AMD instalado

AWSA oferece diferentes imagens de máquina da Amazon (AMI) que vêm com os drivers AMD instalados. Abra [Ofertas do Open Marketplace com o driver AMD](#).

Download do driver AMD

Se você não estiver usando uma AMI com o driver AMD instalado, você pode fazer download do driver AMD e instalá-lo em sua instância.

Esses downloads estão disponíveis somente para clientes da AWS. Ao fazer download, você concorda que usará o software submetido a download somente para desenvolver AMIs para uso com o hardware AMD Radeon Pro V520. Após a instalação do software, você estará vinculado aos termos do [Contrato de licença de usuário final do software AMD](#).

Prerequisites

- Configure as credenciais padrão para o AWS Tools for Windows PowerShell em sua instância do Windows. Para obter mais informações, consulte [Getting Started with the AWS Tools for Windows](#)

[PowerShell](#) (Conceitos básicos do AWS Tools for Windows PowerShell) no AWS Tools for Windows PowerShell User Guide (Manual do usuário do AWS Tools for Windows PowerShell).

- Os usuários do IAM devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess.

Para instalar o driver AMD em sua instância do Windows

1. Conecte-se à instância do Windows e abra uma janela do PowerShell.
2. Faça download dos drivers de Amazon S3 para seu desktop usando os seguintes comandos do PowerShell.

```
$Bucket = "ec2-amd-windows-drivers"
$keyPrefix = "latest"
$localPath = "$home\Desktop\AMD"
$objects = Get-S3Object -BucketName $Bucket -KeyPrefix $keyPrefix -Region us-east-1
foreach ($object in $objects) {
    $localFileName = $object.Key
    if ($localFileName -ne '' -and $object.Size -ne 0) {
        $localFilePath = Join-Path $localPath $localFileName
        Copy-S3Object -BucketName $Bucket -Key $object.Key -LocalFile $localFilePath -Region us-east-1
    }
}
```

3. Descompacte o arquivo de driver obtido por download e execute o instalador usando os comandos do PowerShell a seguir.

```
Expand-Archive $localFilePath -DestinationPath $home\Desktop -Verbose
$driverDir = Get-ChildItem $home\Desktop\ -Directory -Filter "*WHQL*"
Write-Host $driverDir
pnputil /add-driver $home\Desktop\$driverDir\Drivers\Display\WT6A_INF\*inf /install
```

4. Siga as instruções para instalar o driver e reinicialize sua instância, conforme necessário.
5. Para verificar se a GPU está funcionando corretamente, verifique o gerenciador de dispositivos. Você deve ver “AMD Radeon Pro V520 MxGPU” listado como um adaptador de exibição.
6. Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4K, configure o protocolo de exibição de alta performance, [NICE DCV](#).

Ativar NVIDIA GRID Virtual Applications

Para ativar GRID Virtual Applications em instâncias G3 e G4dn (a NVIDIA GRID Virtual Workstation é habilitada por padrão), você deverá definir o tipo de produto para o driver no registro.

Como ativar GRID Virtual Applications em instâncias do Windows

1. Execute regedit.exe para abrir o editor do registro.
2. Navegue até HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global\GridLicensing.
3. Abra o menu de contexto (clique com o botão direito do mouse) no painel direito e escolha New, DWORD.
4. Em Nome, digite FeatureType e Enter.
5. Abra o menu de contexto (clique com o botão direito do mouse) em FeatureType e escolha Modify.
6. Para Dados de valor, insira o para NVIDIA Grid Virtual Applications e escolha OK.
7. Abra o menu de contexto (clique com o botão direito do mouse) no painel direito e escolha New, DWORD.
8. Em Name, digite IgnoreSP e pressione Enter.

9. Abra o menu de contexto (clique com o botão direito do mouse) em IgnoreSP e escolha Modify.
10. Em Value data, digite 1 e escolha OK.
11. Feche o editor de Registro.

Para otimizar as configurações de GPU

Há várias otimizações de configuração de GPU que você pode executar para obter a melhor performance em instâncias G3, G4dn, P2, P3 e P3dn. Com alguns desses tipos de instância, o driver NVIDIA usa um recurso de autoboot, que varia as velocidades de clock da GPU. Ao desativar o recurso de autoboot e definir as velocidades de clock de GPU como a frequência máxima, você pode atingir a performance máxima de forma consistente com suas instâncias de GPU.

Para otimizar as configurações de GPU

1. Abra uma janela do PowerShell e navegue para a pasta de instalação NVIDIA.

```
cd "C:\Program Files\NVIDIA Corporation\NVSMI"
```

2. Instâncias G2, G3 e P2: desative o recurso de autoboot para todas as GPUs na instância.

Note

GPUs em instâncias G4dn, P3 e P3dn não oferecem suporte a autoboot.

```
.\nvidia-smi --auto-boost-default=0
```

3. Defina todas as velocidades de relógio de GPU como a frequência máxima. Use a memória e as velocidades de relógio de placa gráfica especificadas nos seguintes comandos.

Algumas versões do driver NVIDIA não suportam a configuração da velocidade de clock da aplicação e exibem o erro "Setting applications clocks is not supported for GPU...", que você pode ignorar.

- Instâncias G3:

```
.\nvidia-smi -ac "2505,1177"
```

- Instâncias G4dn:

```
.\nvidia-smi -ac "5001,1590"
```

- Instâncias P2:

```
.\nvidia-smi -ac "2505,875"
```

- Instâncias P3 e P3dn:

```
.\nvidia-smi -ac "877,1530"
```

Localizar um tipo de instância do Amazon EC2

Para poder executar uma instância, você deve selecionar um tipo de instância para usar. O tipo de instância escolhido pode depender dos seus requisitos para as instâncias que você executará. Por exemplo, você pode escolher um tipo de instância com base nos seguintes requisitos:

- Zona de disponibilidade ou região
- Computação
- Memória
- Redes
- Definição de preços
- Armazenamento

Localizar um tipo de instância usando o console

É possível encontrar um tipo de instância que atenda às suas necessidades usando o console do Amazon EC2.

Como encontrar um tipo de instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região na qual executar as instâncias. Selecione qualquer região que estiver disponível para você, independentemente do seu local.
3. No painel de navegação, selecione Instance Types (Tipos de instância).
4. (Opcional) Selecione o ícone de preferências (engrenagem) para escolher quais atributos de tipos de instância exibir, como a Definição de preço do Linux sob demanda e selecione Confirmar. Como alternativa, escolha um tipo de instância e visualize todos os atributos usando o painel Detalhes.
5. Use os atributos de tipo de instância para filtrar a lista de tipos de instância exibidos apenas para os tipos de instância que atendem às suas necessidades. Por exemplo, é possível listar todos os tipos de instância que têm mais de oito vCPUs e que também oferecem suporte à hibernação.
6. (Opcional) Selecione vários tipos de instâncias para ver uma comparação lado a lado entre todos os atributos no painel Details (Detalhes).
7. (Opcional) Para salvar a lista de tipos de instância em um arquivo de valores separados por vírgulas (.csv) para revisão adicional, selecione Fazer download da lista CSV. O arquivo inclui todos os tipos de instância que correspondem aos filtros definidos.
8. Depois de localizar tipos de instância que atendam às suas necessidades, você pode usá-los para executar instâncias. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).

Localizar um tipo de instância usando a AWS CLI

É possível usar comandos da AWS CLI para que o Amazon EC2 encontrar um tipo de instância que atenda às suas necessidades.

Como encontrar um tipo de instância usando a AWS CLI

1. Se ainda não o tiver feito isso, instale a AWS CLI. Para obter mais informações, consulte o [AWS Command Line Interface User Guide](#) (Manual do usuário da AWS Command Line Interface).
2. Use o comando `describe-instance-types` para filtrar tipos de instância com base em atributos de instância. Por exemplo, é possível usar o comando a seguir para exibir somente os tipos de instância com 48 vCPUs.

```
aws ec2 describe-instance-types --filters "Name=vcpu-info.default-vcpus,Values=48"
```

3. Use o comando `describe-instance-type-offerings` para filtrar os tipos de instância oferecidos por local (região ou zona de disponibilidade). Por exemplo, é possível usar o comando a seguir para exibir os tipos de instância oferecidos na zona de disponibilidade especificada.

```
aws ec2 describe-instance-type-offerings --location-type "availability-zone" --filters Name=location,Values=us-east-2a --region us-east-2
```

- Depois de localizar tipos de instância que atendam às suas necessidades, anote-os para que você possa usar esses tipos de instância ao executar instâncias. Para obter mais informações, consulte [Launching your instance](#) (Iniciar sua instância) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).

Alterar o tipo de instância

À medida que suas necessidades mudarem, você pode descobrir que a instância está sobreutilizada (o tipo de instância é muito pequeno) ou subutilizada (o tipo de instância é muito grande). Se esse for o caso, você poderá redimensionar a sua instância alterando o seu tipo de instância. Por exemplo, se a instância `t2.micro` for muito pequena para sua workload, você poderá alterá-la para outra tipo de instância apropriado para a workload.

Você também pode migrar de um tipo de instância de geração anterior para um tipo de instância de geração atual para aproveitar alguns recursos, por exemplo, suporte para IPv6.

Se você quiser uma recomendação para um tipo de instância que esteja mais apto a lidar com sua workload existente, você pode usar o AWS Compute Optimizer. Para obter mais informações, consulte [Obter recomendações de um tipo de instância \(p. 249\)](#).

Tópicos

- [Requisitos para alterar os tipos de instância \(p. 244\)](#)
- [Compatibilidade para alterar o tipo de instância \(p. 244\)](#)
- [Alterar o tipo de instância de uma instância com Amazon EBS \(p. 245\)](#)
- [Migrar para uma nova configuração de instância \(p. 248\)](#)

Requisitos para alterar os tipos de instância

Para redimensionar a instância do Amazon EC2 alterando o tipo de instância, considere os seguintes requisitos:

- Você deve selecionar um tipo de instância que seja compatível com a configuração da instância. Se o tipo da instância desejada não for compatível com a configuração da instância que você tem, migre a aplicação para uma nova instância com o tipo de instância de que você precisa.
- Para alterar o tipo de instância, a instância deve estar no estado `stopped`.
- Não é possível redimensionar uma instância se a hibernação estiver ativada.

Compatibilidade para alterar o tipo de instância

Você pode redimensionar uma instância somente se o tipo da instância atual e o novo tipo de instância desejado forem compatíveis das seguintes formas:

- Arquitetura: as AMIs são específicas à arquitetura do processador, portanto, você deve selecionar um tipo de instância com a mesma arquitetura do processador como o tipo da instância atual. Por exemplo:
 - Se estiver redimensionando um tipo de instância com um processador com base na arquitetura do Arm, você estará limitado aos tipos de instância que oferecem suporte a um processador com base na arquitetura do Arm, como o C6g e M6g.
- Os seguintes tipos de instância são os únicos tipos de instância que oferecem suporte a AMIs de 32 bits: `t2.nano`, `t2.micro`, `t2.small`, `t2.medium`, `c3.large`, `t1.micro`, `m1.small`, `m1.medium`

e c1.medium. Se estiver redimensionando uma instância de 32 bits, você estará limitado a esses tipos de instância.

- Network: Tipos de instâncias mais novos devem ser executados em uma VPC. Portanto, não é possível redimensionar uma instância na plataforma do EC2-Classic para um tipo de instância que esteja disponível somente em uma VPC a menos que você tenha uma VPC não padrão. Para verificar se a instância está em uma VPC, verifique o valor de VPC ID no painel de detalhes da tela Instances no console do Amazon EC2. Para obter mais informações, consulte [Migre do EC2-Classic para uma VPC \(p. 1119\)](#).
- Adaptadores de rede: se você alternar de um driver de um adaptador de rede para outro, as configurações do adaptador de rede serão redefinidas quando o sistema operacional criar o novo adaptador. Para redefinir as configurações, talvez seja necessário ter acesso a uma conta local com permissões de administrador. Veja a seguir exemplos de mudança de um adaptador de rede para outro:
 - AWS PV (instâncias T2) para Intel 82599 VF (instâncias M4)
 - Intel 82599 VF (maioria das instâncias M4) para ENA (instâncias M5)
 - ENA (instâncias M5) para ENA de alta largura de banda (instâncias M5n)
- Redes aprimoradas: tipos de instância que dão suporte a [redes aprimoradas \(p. 1028\)](#) exigem os drivers necessários instalados. Por exemplo, as instâncias baseadas no [Sistema Nitro \(p. 154\)](#) precisam de AMIs baseadas no EBS com os drivers do Elastic Network Adapter (ENA) instalados. Para redimensionar uma instância de um tipo que não oferece suporte à rede avançada para um tipo que ofereça suporte à rede avançada, é necessário instalar os [drivers do ENA \(p. 1029\)](#) ou os [drivers ixgbevf \(p. 1037\)](#) na instância, conforme apropriado.
- NVMe: os volumes do EBS são expostos como dispositivos de blocos NVMe em instâncias criadas no [sistema Nitro \(p. 154\)](#). Se você redimensionar uma instância de um tipo de instância não compatível com NVMe para um tipo de instância compatível com NVMe, deverá primeiro instalar os [drivers NVMe \(p. 1438\)](#) em sua instância. Além disso, os nomes de dispositivo que você especifica no mapeamento de dispositivos de blocos são renomeados usando nomes de dispositivo de NVMe (/dev/nvme[0-26]n1).
- AMI: Para obter informações sobre as AMIs exigidas por tipos de instância que suportam rede aperfeiçoada e NVMe, consulte as notas de release na seguinte documentação:
 - [Instâncias de uso geral \(p. 158\)](#)
 - [Instâncias otimizadas para computação \(p. 204\)](#)
 - [Instâncias otimizadas para memória \(p. 211\)](#)
 - [Instâncias otimizadas para armazenamento \(p. 222\)](#)

Alterar o tipo de instância de uma instância com Amazon EBS

Considerações

Você deve interromper sua instância com Amazon EBS para poder alterar o tipo da instância. Ao parar e iniciar uma instância, esteja ciente do seguinte:

- Movemos a instância para um novo hardware. No entanto, o ID da instância não é alterado.
- Se sua instância tiver um endereço IPv4 público, nós liberamos o endereço e damos a ele um novo endereço IPv4 público. A instância retém seus endereços IPv4 privados, todos os endereços IP elásticos e todos os endereços IPv6.
- Quando você redimensiona uma instância, a instância redimensionada tem o mesmo número de volumes de armazenamento da instância que você especificou ao executar a instância original. Com tipos de instância que são compatíveis com volumes de armazenamento de instâncias NVMe (disponíveis por padrão), a instância redimensionada pode ter volumes adicionais de armazenamento de instâncias, dependendo da AMI. Caso contrário, você pode migrar sua aplicação para uma instância com um novo tipo de instância manualmente, especificando o número de volumes de armazenamento de instâncias necessários ao iniciar a nova instância.

- Se sua instância estiver em um grupo do Auto Scaling, o serviço do Amazon EC2 Auto Scaling marcará a instância interrompida como não íntegra e poderá encerrá-la e executar uma instância substituta. Para evitar isso, você poderá suspender os processos de escalabilidade para o grupo enquanto estiver redimensionando a instância. Para obter mais informações, consulte [Suspensão e retomada dos processos de escalabilidade](#) no Guia do usuário do Amazon EC2 Auto Scaling.
- Se a instância estiver em um [placement group de cluster](#) (p. 1044) e, após alterar o tipo da instância, esta começar a falhar, tente fazer o seguinte: interrompa todas as instâncias do placement group de cluster, altere o tipo da instância afetada e reinicie todas as instâncias do placement group do cluster.
- Planeje tempo de inatividade enquanto a instância estiver parada. A parada e o redimensionamento de uma instância pode levar alguns minutos, e o reinício da instância pode levar uma quantidade variável de tempo dependendo dos scripts de startup da aplicação.

Para obter mais informações, consulte [Interromper e iniciar sua instância](#) (p. 455).

Alterar o tipo de instância

Use o procedimento a seguir para alterar um tipo de instância com Amazon EBS usando o AWS Management Console.

New console

Para alterar o tipo de instância de uma instância com Amazon EBS

1. (Opcional) Se o tipo de instância requer drivers que não estejam instalados na instância atual, você deve se conectar à sua instância e instalar os drivers primeiro. Para obter mais informações, consulte [Compatibilidade para alterar o tipo de instância](#) (p. 244).

Note

O pacote do driver AWS PV deve ser atualizado antes da alteração de famílias de instâncias. Para obter mais informações, consulte [Atualizar drivers de PV em instâncias do Windows](#) (p. 565).

2. (Opcional) Se você configurou a instância do Windows para usar [endereçamento IP estático](#) (p. 610) e redimensionar a instância de um tipo não compatível com redes avançadas para um tipo de instância compatível com redes avançadas, poderá receber um aviso sobre um possível conflito de endereços IP ao reconfigurar o endereçamento IP estático. Para evitar isso, habilite o DHCP na interface de rede da instância antes de alterar o tipo de instância. Na instância, abra a Central de rede e compartilhamento, vá para Propriedades do protocolo IP versão 4 (TCP/IPv4) para a interface de rede e escolha Obter um endereço IP automaticamente. Altere o tipo de instância e reconfigure o endereçamento IP estático na interface de rede.
3. Abra o console do Amazon EC2.
4. [Windows Server 2016 e posterior] Conecte-se à instância do Windows e execute o seguinte script do PowerShell do EC2Launch para configurar a instância após ela ter sido redimensionada.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

5. No painel de navegação, escolha Instances (Instâncias).
6. Selecione a instância e escolha Actions (Ações), Instance state (Estado da instância) e Stop instance (Interromper instância).
7. Na caixa de diálogo de confirmação, escolha Stop (Interromper). Pode demorar alguns minutos para que a instância pare.
8. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Change instance type (Alterar tipo de instância). Essa ação estará acinzentada se o estado da instância não for stopped.
9. Na caixa de diálogo Change instance type (Alterar tipo de instância), faça o seguinte:

- a. Em Instance type (Tipo de instância), selecione o tipo de instância desejado. Se o tipo de instância desejado não aparecer na lista, ele não será compatível com a configuração da instância (por exemplo, devido ao tipo de virtualização). Para obter mais informações, consulte [Compatibilidade para alterar o tipo de instância \(p. 244\)](#).
 - b. (Opcional) Se o tipo de instância selecionado oferecer suporte a otimização para EBS, selecione EBS-optimized (Optimizado para EBS) ou desmarque a opção EBS-optimized (Optimizado para EBS) para desativar a otimização para EBS. Se, por padrão, o tipo de instância selecionado for otimizada para EBS, a opção EBS-optimized (Optimizada para EBS) estará selecionada e você não poderá desmarcá-la.
 - c. Escolha Apply para aceitar as novas configurações.
10. Para reiniciar a instância interrompida, selecione a instância e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Pode demorar alguns minutos para que a instância entre no estado `running`.

Old console

Para alterar o tipo de instância de uma instância com Amazon EBS

1. (Opcional) Se o tipo de instância requer drivers que não estejam instalados na instância atual, você deve se conectar à sua instância e instalar os drivers primeiro. Para obter mais informações, consulte [Compatibilidade para alterar o tipo de instância \(p. 244\)](#).

Note

O pacote do driver AWS PV deve ser atualizado antes da alteração de famílias de instâncias. Para obter mais informações, consulte [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#).

2. (Opcional) Se você configurou a instância do Windows para usar [endereçamento IP estático \(p. 610\)](#) e redimensionar a instância de um tipo não compatível com redes avançadas para um tipo de instância compatível com redes avançadas, poderá receber um aviso sobre um possível conflito de endereços IP ao reconfigurar o endereçamento IP estático. Para evitar isso, habilite o DHCP na interface de rede da instância antes de alterar o tipo de instância. Na instância, abra a Central de rede e compartilhamento, vá para Propriedades do protocolo IP versão 4 (TCP/IPv4) para a interface de rede e escolha Obter um endereço IP automaticamente. Altere o tipo de instância e reconfigure o endereçamento IP estático na interface de rede.
3. Abra o console do Amazon EC2.
4. [Windows Server 2016 e posterior] Conecte-se à instância do Windows e execute o seguinte script do PowerShell do EC2Launch para configurar a instância após ela ter sido redimensionada.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -  
Schedule
```

5. No painel de navegação, escolha Instances (Instâncias).
6. Selecione a instância e escolha Actions, Instance State e Stop.
7. Na caixa de diálogo para confirmação, escolha Yes, parar. Pode demorar alguns minutos para que a instância pare.
8. Com a instância ainda selecionada, escolha Ações, Instance Settings, Change Instance Type. Essa ação estará acinzentada se o estado da instância não for stopped.
9. Na caixa de diálogo Change Instance Type, faça o seguinte:
 - a. Em Instance Type, selecione o tipo de instância desejado. Se o tipo de instância desejado não aparecer na lista, ele não será compatível com a configuração da instância (por exemplo, devido ao tipo de virtualização). Para obter mais informações, consulte [Compatibilidade para alterar o tipo de instância \(p. 244\)](#).

- b. (Opcional) Se o tipo de instância selecionado oferecer suporte a otimização para EBS, selecione EBS-optimized (Optimizado para EBS) ou desmarque a opção EBS-optimized (Optimizado para EBS) para desativar a otimização para EBS. Se, por padrão, o tipo de instância selecionado for otimizada para EBS, a opção EBS-optimized (Optimizada para EBS) estará selecionada e você não poderá desmarcá-la.
 - c. Escolha Apply para aceitar as novas configurações.
10. Para reiniciar a instância interrompida, selecione a instância e escolha Ações, Instance State, Iniciar.
11. Na caixa de diálogo de confirmação, escolha Sim, iniciar. Pode demorar alguns minutos para que a instância entre no estado `running`.

Migrar para uma nova configuração de instância

Se a configuração atual da instância não for compatível com o novo tipo de instância desejado, não será possível redimensionar a instância para aquele tipo de instância. Em vez disso, é possível migrar sua aplicação para uma nova instância com uma configuração que seja compatível com o novo tipo de instância desejado.

New console

Para migrar a aplicação para uma instância compatível

1. Faça backup de todos os dados nos volumes de armazenamento de instâncias necessários para manter o armazenamento persistente. Para migrar dados nos volumes do EBS que você precisa manter, crie um snapshot dos volumes (consulte [Criar snapshots de Amazon EBS \(p. 1298\)](#)) ou desanexe o volume da instância para que você possa anexá-lo à nova instância mais tarde (consulte [Desanexar um volume do Amazon EBS de uma instância Windows \(p. 1290\)](#)).
2. Execute uma nova instância selecionando o seguinte:
 - Se estiver usando um endereço IP elástico, selecione a VPC na qual a instância original está em execução.
 - Todos os volumes do EBS que você desanexou da instância original e quer anexar à nova instância ou os novos volumes do EBS baseados nos snapshots que você criou.
 - Para permitir que algum tráfego atinja a nova instância, selecione o security group que está associado à instância original.
3. Instale a aplicação e qualquer software necessário na instância.
4. Restaure todos os dados dos quais você fez backup dos volumes de armazenamento de instâncias da instância original.
5. Se estiver usando um endereço IP elástico, atribua-o à instância recém-executada da seguinte forma:
 - a. No painel de navegação, escolha Elastic IPs.
 - b. Selecione o endereço IP elástico que está associado à instância original e escolha Actions (Ações) e Disassociate Elastic IP address (Desassociar endereço IP elástico). Quando a confirmação for solicitada, escolha Disassociate (Desassociar).
 - c. Com o endereço IP elástico ainda selecionado, escolha Actions (Ações) e Associate Elastic IP address (Associar endereço IP elástico).
 - d. Em Resource type (Tipo de recurso), escolha Instance (Instância).
 - e. Em Instance (Instância), escolha a instância à qual associar o endereço IP elástico. Você também pode inserir texto para pesquisar uma instância específica.
 - f. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.
 - g. Escolha Associate.

6. (Opcional) Você pode encerrar a instância original se ela não for mais necessária. Selecione a instância e verifique se você está prestes a encerrar a instância original e não a nova instância (por exemplo, verifique o nome ou a hora da execução). Escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Old console

Para migrar o aplicativo para uma instância compatível

1. Faça backup de todos os dados nos volumes de armazenamento de instâncias necessários para manter o armazenamento persistente. Para migrar dados nos volumes do EBS que você precisa manter, crie um snapshot dos volumes (consulte [Criar snapshots de Amazon EBS \(p. 1298\)](#)) ou desanexe o volume da instância para que você possa anexá-lo à nova instância mais tarde (consulte [Desanexar um volume do Amazon EBS de uma instância Windows \(p. 1290\)](#)).
2. Execute uma nova instância selecionando o seguinte:
 - Se estiver usando um endereço IP elástico, selecione a VPC na qual a instância original está em execução.
 - Todos os volumes do EBS que você desanexou da instância original e quer anexar à nova instância ou os novos volumes do EBS baseados nos snapshots que você criou.
 - Para permitir que algum tráfego atinja a nova instância, selecione o security group que está associado à instância original.
3. Instale a aplicação e qualquer software necessário na instância.
4. Restaure todos os dados dos quais você fez backup dos volumes de armazenamento de instâncias da instância original.
5. Se estiver usando um endereço IP elástico, atribua-o à instância recém-executada da seguinte forma:
 - a. No painel de navegação, escolha Elastic IPs.
 - b. Selecione o endereço IP elástico que está associado à instância original e escolha Actions (Ações) e Disassociate address (Desassociar endereço). Quando a confirmação for solicitada, escolha Disassociate address.
 - c. Com o endereço IP elástico ainda selecionado, escolha Actions (Ações) e Associate address (Associar endereço).
 - d. Em Instance, selecione a nova instância e escolha Associate.
6. (Opcional) Você pode encerrar a instância original se ela não for mais necessária. Selecione a instância e verifique se você está prestes a encerrar a instância original e não a nova instância (por exemplo, verifique o nome ou a hora da execução). Escolha Actions (Ações), Instance State (Estado da instância), Terminate (Encerrar).

Obter recomendações de um tipo de instância

O AWS Compute Optimizer fornece recomendações para instâncias do Amazon EC2 para ajudar a melhorar a performance, economizar dinheiro ou ambos. É possível usar essas recomendações para decidir se deseja passar para um novo tipo de instância.

Para fazer recomendações, o Compute Optimizer analisa as especificações de instância existentes e as métricas de utilização. Os dados compilados são usados para recomendar quais tipos de instância do Amazon EC2 são melhores para lidar com a workload existente. As recomendações são retornadas com a definição de preço de instância por hora.

Este tópico descreve como visualizar as recomendações por meio do console do Amazon EC2. Para obter mais informações, consulte o [Guia do usuário do AWS Compute Optimizer](#).

Note

Para obter recomendações do Compute Optimizer, primeiro é necessário optar pelo Compute Optimizer. Para obter mais informações, consulte [Getting Started with AWS Compute Optimizer](#) (Conceitos básicos do AWS Compute Optimizer) no AWS Compute Optimizer User Guide (Manual do usuário do AWS Compute Optimizer).

Tópicos

- [Limitations \(p. 250\)](#)
- [Findings \(p. 250\)](#)
- [Exibir recomendações \(p. 250\)](#)
- [Considerações para avaliação das recomendações \(p. 252\)](#)
- [Recursos adicionais \(p. 253\)](#)

Limitations

Atualmente, o Compute Optimizer gera recomendações para os tipos de instância M, C, R, T e X. Outros tipos de instância não são considerados pelo Compute Optimizer. Se estiver usando outros tipos de instância, eles não serão listados na visualização de recomendações do Compute Optimizer. Para obter informações sobre esses e outros tipos de instância, consulte [Tipos de instância \(p. 149\)](#).

Findings

O Compute Optimizer classifica suas descobertas para instâncias do EC2 da seguinte forma:

- Under-provisioned (Subprovisionada) – uma instância do EC2 será considerada subprovisionada quando pelo menos uma especificação, como CPU, memória ou rede, não atender aos requisitos de performance de sua workload. Instâncias do EC2 subprovisionadas podem gerar performance ruim da aplicação.
- Over-provisioned (Superprovisionada) – uma instância do EC2 será considerada superprovisionada quando pelo menos uma especificação, como CPU, memória ou rede, puder ser reduzida sem deixar de atender aos requisitos de performance de sua workload e quando nenhuma especificação estiver subprovisionada. Instâncias do EC2 superprovisionadas podem gerar custos desnecessários de infraestrutura.
- Optimized (Otimizada) – uma instância do EC2 será considerada otimizada quando todas as especificações, como CPU, memória e rede, atenderem aos requisitos de performance de sua workload e a instância não estiver superprovisionada. Uma instância do EC2 otimizada executa suas workloads com performance e custo de infraestrutura ideais. Para instâncias otimizadas, o Compute Optimizer às vezes pode recomendar um tipo de instância de nova geração.
- None (Nenhum) – não há recomendações para essa instância. Isso pode ocorrer se você tiver optado pelo Compute Optimizer há menos de 12 horas, quando a instância estiver sendo executada há menos de 30 horas ou quando o tipo de instância não for compatível com o Compute Optimizer. Para obter mais informações, consulte [Limitations \(p. 250\)](#) na seção anterior.

Exibir recomendações

Depois de optar pelo Compute Optimizer, será possível visualizar as descobertas que Compute Optimizer gera para suas instâncias do EC2 no console do EC2. Depois, você poderá acessar o console do Compute Optimizer para visualizar as recomendações. Caso tenha realizado a opção recentemente, as descobertas poderão não ser refletidas no console do EC2 durante até 12 horas.

New console

Como visualizar uma recomendação para uma instância do EC2 por meio do console do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias) e selecione o ID da instância.
3. Na página de resumo da instância, no banner do AWS Compute Optimizer, próximo à parte inferior da página, escolha View detail (Visualizar detalhes).

A instância será aberta no Compute Optimizer, onde ela será rotulada como a instância Current (Atual). Até três recomendações de tipo de instância diferentes, rotuladas como Option 1 (Opção 1), Option 2 (Opção 2) e Option 3 (Opção 3), serão fornecidas. A metade inferior da janela mostra dados recentes de métricas do CloudWatch para a instância atual: CPU utilization (Uso da CPU), Memory utilization (Uso da memória), Network in (Entrada da rede) e Network out (Saída da rede).

4. (Opcional) No console do Compute Optimizer, escolha o ícone de configurações ( para alterar as colunas visíveis na tabela ou para visualizar as informações públicas de definição de preço a fim de obter uma opção de compra diferente para os tipos de instância atuais e recomendados.

Note

Se você comprou uma Instância reservada, sua instância sob demanda poderá ser cobrada como uma Instância reservada. Antes de alterar o tipo de instância atual, avalie o impacto sobre o uso e a cobertura da Instância reservada.

Old console

Como visualizar uma recomendação para uma instância do EC2 por meio do console do EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e, na guia Description (Descrição), inspecione o campo Finding (Descoberta). Escolha View detail (Exibir detalhes).

A instância será aberta no Compute Optimizer, onde ela será rotulada como a instância Current (Atual). Até três recomendações de tipo de instância diferentes, rotuladas como Option 1 (Opção 1), Option 2 (Opção 2) e Option 3 (Opção 3), serão fornecidas. A metade inferior da janela mostra dados recentes de métricas do CloudWatch para a instância atual: CPU utilization (Uso da CPU), Memory utilization (Uso da memória), Network in (Entrada da rede) e Network out (Saída da rede).

4. (Opcional) No console do Compute Optimizer, escolha o ícone de configurações ( para alterar as colunas visíveis na tabela ou para visualizar as informações públicas de definição de preço a fim de obter uma opção de compra diferente para os tipos de instância atuais e recomendados.

Note

Se você comprou uma Instância reservada, sua instância sob demanda poderá ser cobrada como uma Instância reservada. Antes de alterar o tipo de instância atual, avalie o impacto sobre o uso e a cobertura da Instância reservada.

Determine se deseja usar uma das recomendações. Decida se deseja otimizar para melhorar a performance, reduzir custos ou uma combinação dos dois. Para obter mais informações, consulte [Visualizar recomendações de recursos](#) no AWS Compute OptimizerGuia do usuário do AWS Compute Optimizer.

Como visualizar as recomendações para todas as instâncias do EC2 em todas as regiões no console do Compute Optimizer

1. Abra o console do Compute Optimizer em <https://console.aws.amazon.com/compute-optimizer/>.
2. Escolha View recommendations for all EC2 instances (Exibir recomendações para todas as instâncias do EC2).
3. É possível executar as seguintes ações na página de recomendações:
 - a. Para filtrar recomendações para uma ou mais regiões da AWS, insira o nome da região na caixa de texto Filter by one or more Regions (Filtrar por uma ou mais regiões) ou escolha uma ou mais regiões na lista suspensa exibida.
 - b. Para visualizar as recomendações para recursos em outra conta, escolha Account (Conta) e selecione um ID de conta diferente.

Essa opção estará disponível somente se você estiver conectado a conta de gerenciamento de uma organização e tiver optado por todas as contas-membros da organização.
 - c. Para limpar os filtros selecionados, escolha Clear filters (Limpar filtros).
 - d. Para alterar a opção de compra exibida para os tipos de instância atuais e recomendados, escolha o ícone de configurações () e selecione On-Demand Instances (Instâncias sob demanda), Reserved Instances, standard 1-year no upfront (Instâncias reservadas, padrão de 1 ano sem adiantamento) ou Reserved Instances, standard 3-year no upfront (Instâncias reservadas, padrão de 3 anos sem adiantamento).
 - e. Para exibir detalhes, como recomendações adicionais e uma comparação das métricas de utilização, escolha a descoberta (Under-provisioned (Subprovisionada), Over-provisioned (Superprovisionada) ou Optimized (Otimizada)) listada ao lado da instância desejada. Para obter mais informações, consulte [Viewing Resource Details](#) (Visualizar detalhes do recurso) no AWS Compute Optimizer User Guide (Manual do usuário do AWS Compute Optimizer).

Considerações para avaliação das recomendações

Antes de alterar um tipo de instância, considere o seguinte:

- As recomendações não preveem seu uso. As recomendações são baseadas em seu histórico de uso durante os últimos 14 dias. Escolha um tipo de instância que tenha a expectativa de atender às suas necessidades futuras de recursos.
- Concentre-se nas métricas gráficas para determinar se o uso real é menor do que a capacidade da instância. Também é possível exibir dados de métricas (média, pico, percentil) no CloudWatch para aprofundar a avaliação de suas recomendações de instâncias do EC2. Por exemplo, observe como as métricas de porcentagem da CPU mudam durante o dia e se há picos que precisem ser acomodados. Para obter mais informações, consulte [Visualizar métricas disponíveis](#) no Guia do usuário do Amazon CloudWatch.
- O Compute Optimizer pode fornecer recomendações para instâncias expansíveis, que são as instâncias T3, T3a e T2. Se você ultrapassa periodicamente a linha de base, verifique se poderá continuar a fazer isso com base nas vCPUs do novo tipo de instância. Para obter mais informações, consulte [Principais conceitos e definições para instâncias expansíveis \(p. 171\)](#).
- Se você comprou uma Instância reservada, sua instância sob demanda poderá ser cobrada como uma Instância reservada. Antes de alterar o tipo de instância atual, avalie o impacto sobre o uso e a cobertura da Instância reservada.
- Considere conversões para instâncias da geração mais recente, sempre que possível.
- Ao migrar para uma família de instâncias diferente, verifique se o tipo de instância atual e o novo tipo de instância são compatíveis, por exemplo, em termos de virtualização, arquitetura ou tipo de rede. Para obter mais informações, consulte [Compatibilidade para alterar o tipo de instância \(p. 244\)](#).

- Por fim, considere a classificação de risco de performance fornecida para cada recomendação. O risco de performance indica o esforço necessário para validar se o tipo de instância recomendado atende aos requisitos de performance da sua workload. Também recomendamos testes rigorosos de carga e performance antes e depois de fazer quaisquer alterações.

Há outras considerações ao redimensionar uma instância do EC2. Para obter mais informações, consulte [Alterar o tipo de instância \(p. 244\)](#).

Recursos adicionais

Para obter mais informações:

- [Tipos de instância \(p. 149\)](#)
- [AWS Compute Optimizer Guia do usuário](#)

Opções de compra de instância

O Amazon EC2 fornece as seguintes opções de compra para permitir otimizar os custos com base em suas necessidades:

- Instâncias sob demanda: pague pelas instâncias que você iniciar
- Savings Plans: reduza os custos do Amazon EC2 se comprometendo com uma quantidade consistente de uso, em USD por hora, por um período de vigência de um ou de três anos.
- Reserved Instances (Instâncias reservadas): reduza os custos do Amazon EC2 se comprometendo com uma configuração consistente de instância, incluindo o tipo de instância e a região, por um período de vigência de um ou de três anos.
- Spot Instances (Instâncias spot): solicite instâncias do EC2 não utilizadas, o que pode reduzir os custos do Amazon EC2 significativamente.
- Dedicated Hosts (Hosts dedicados): pague por um host físico que seja totalmente dedicado à execução de suas instâncias e traga suas licenças de software existentes por soquete, por núcleo ou por VM para reduzir custos.
- Dedicated Instances (Instâncias dedicadas): pague por hora pelas instâncias que são executadas no hardware de um ocupante único.
- Capacity Reservations (Reservas de Capacidade): reserve capacidade para suas instâncias do EC2 em uma zona de disponibilidade específica por qualquer duração.

Se você precisar de uma reserva de capacidade, compre instâncias reservadas ou Reservas de Capacidade para uma zona de disponibilidade específica. As instâncias spot são uma opção econômica se houver flexibilidade quanto ao momento em que as aplicações serão executados e se poderão ser interrompidas. Os hosts dedicados ou as instâncias dedicadas podem ajudar você a atender aos requisitos de conformidade e reduzir custos usando as licenças de software associadas ao servidor. Para obter mais informações, consulte [Definição de preço Amazon EC2](#).

Para obter mais informações sobre Savings Plans, consulte o [Guia do usuário do AWS Savings Plans](#).

Tópicos

- [Determinar o ciclo de vida da instância \(p. 254\)](#)
- [On-Demand Instances \(p. 255\)](#)
- [Reserved Instances \(p. 259\)](#)
- [Scheduled Reserved Instances \(p. 298\)](#)

- [Spot Instances \(p. 299\)](#)
- [Dedicated Hosts \(p. 349\)](#)
- [Dedicated Instances \(p. 383\)](#)
- [On-Demand Capacity Reservations \(p. 390\)](#)

Determinar o ciclo de vida da instância

O ciclo de vida de uma instância começa quando ela é executada e termina quando é encerrada. A opção de compra escolhida afeta o ciclo de vida da instância. Por exemplo, uma instância sob demanda é executada quando você a inicia e é encerrada quando você a encerra. Uma instância spot é executada contanto que sua capacidade esteja disponível e sua sugestão de preço máximo seja superior ao preço spot.

Use o seguinte procedimento para determinar o ciclo de vida de uma instância.

New console

Para determinar o ciclo de vida da instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Details (Detalhes), em Instance details (Detalhes da instância), localize Lifecycle (Ciclo de vida). Se o valor for spot, a instância será uma instância spot. Se o valor for normal, a instância será uma instância sob demanda ou uma Instância reservada.
5. Na guia Details (Detalhes), em Host and placement group (Host e placement group), localize Tenancy (Locação). Se o valor for host, a instância estará em execução em um Host dedicado. Se o valor for dedicated, a instância será uma Instâncias dedicadas.
6. (Opcional) Se você adquiriu uma Instância reservada e deseja verificar se ela está sendo aplicada, poderá verificar os relatórios de uso do Amazon EC2. Para obter mais informações, consulte [Relatórios de uso do Amazon EC2 \(p. 1569\)](#).

Old console

Para determinar o ciclo de vida da instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Description (Descrição), localize Tenancy (Locação). Se o valor for host, a instância estará em execução em um Host dedicado. Se o valor for dedicated, a instância será uma Instâncias dedicadas.
5. Na guia Description (Descrição), localize Lifecycle (Ciclo de vida). Se o valor for spot, a instância será uma instância spot. Se o valor for normal, a instância será uma instância sob demanda ou uma Instância reservada.
6. (Opcional) Se você adquiriu uma Instância reservada e deseja verificar se ela está sendo aplicada, poderá verificar os relatórios de uso do Amazon EC2. Para obter mais informações, consulte [Relatórios de uso do Amazon EC2 \(p. 1569\)](#).

Para determinar o ciclo de vida da instância usando a AWS CLI

Use o seguinte comando [describe-instances](#):

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0
```

Se a instância estiver em execução em um Host dedicado, o resultado conterá as seguintes informações:

```
"Tenancy": "host"
```

Se a instância for uma Instâncias dedicadas, o resultado conterá as seguintes informações:

```
"Tenancy": "dedicated"
```

Se a instância for uma instância spot, o resultado conterá as seguintes informações:

```
"InstanceLifecycle": "spot"
```

Caso contrário, o resultado não conterá `InstanceLifecycle`.

On-Demand Instances

Com o Instâncias on-demand, você paga pela capacidade computacional pela hora, sem nenhum compromisso em longo prazo. Você tem pleno controle sobre o ciclo de vida dela — você decide quando executar, interromper, hibernar, iniciar, reiniciar ou encerrá-la.

Não há compromisso de longo prazo ao comprar Instâncias on-demand. Você paga apenas pelos horas que suas Instâncias on-demand estiverem no estado `running`. O preço por hora para uma instância sob demanda em execução é fixo e está listado na [página Definição de preço do Amazon EC2](#), [Definição de preço sob demanda](#).

Recomendamos o uso de Instâncias on-demand para aplicações com workloads de curto prazo e irregulares que não podem ser interrompidas.

Para economias significativas com relação a instâncias sob demanda, use [AWS Savings Plans](#), [Spot Instances](#) (p. 299) ou [Reserved Instances](#) (p. 259).

Sumário

- [Trabalhar com Instâncias on-demand \(p. 255\)](#)
- [Limites de instância sob demanda \(p. 256\)](#)
 - [Calcular quantas vCPUs você precisa \(p. 256\)](#)
 - [Solicitar um aumento de limite de \(p. 258\)](#)
 - [Monitorar limites e uso de instância sob demanda \(p. 258\)](#)
- [Consulte os preços das instâncias sob demanda \(p. 258\)](#)

Trabalhar com Instâncias on-demand

Você pode trabalhar com Instâncias on-demand das seguintes formas:

- [Executar sua instância \(p. 417\)](#)
- [Conectar-se à sua instância do Windows \(p. 443\)](#)
- [Interromper e iniciar sua instância \(p. 455\)](#)

- Hibernar a instância do Linux sob demanda ou reservada (p. 459)
- Reinicializar a instância (p. 470)
- Desativação da instância (p. 471)
- Encerrar a instância (p. 474)
- Recuperar a instância (p. 480)
- Configurar sua instância do Windows (p. 482)
- Identificar as instâncias do Windows do EC2 (p. 702)

Se você é novo com o Amazon EC2, consulte [Como começar a usar o Amazon EC2 \(p. 2\)](#).

Limites de instância sob demanda

Há um limite para o número de instâncias sob demanda em execução por conta da AWS por Região. Os limites de instância sob demanda são gerenciados em termos do número de unidades de processamento central virtual (vCPUs) que as instâncias sob demanda em execução estão usando, independentemente do tipo de instância.

A tabela a seguir lista os limites de instâncias sob demanda. Cada limite especifica as vCPUs para uma ou mais famílias de instâncias. Para obter informações sobre as diferentes famílias, gerações e tamanhos de instâncias, consulte [Tipos de instância do Amazon EC2](#).

Note

As novas contas da AWS podem começar com limites mais baixos que os desses padrões. O Amazon EC2 monitora seu uso e eleva seus limites automaticamente com base nele.

Limit	vCPUs padrão
Execução de todas as instâncias padrão sob demanda (A, C, D, H, I, M, R, T, Z)	1.152
Execução de todas as instâncias F sob demanda	128
Execução de todas as instâncias G sob demanda	128
Executar instâncias sob demanda com alta memória (u-*)	448
Execução de todas as instâncias Inf sob demanda	128
Execução de todas as instâncias P sob demanda	128
Execução de todas as instâncias X sob demanda	128

Você pode executar qualquer combinação de tipos de instância que atenda às necessidades em constante mudança da sua aplicação, desde que o número de vCPUs não exceda o limite da sua conta. Por exemplo: com um limite de instância padrão de 256 vCPUs, você pode executar 32 instâncias `m5.2xlarge` (32 x 8 vCPUs) ou 16 instâncias `c5.4xlarge` (16 x 16 vCPUs). Para mais informações, consulte [Limites de instância sob demanda do EC2](#).

Calcular quantas vCPUs você precisa

Você pode usar a calculadora de limite de vCPU para determinar o número de vCPUs de que sua aplicação precisa.

Ao usar a calculadora, lembre-se de que: a calculadora presume que você atingiu o limite atual. O valor inserido para Instance count (Contagem de instâncias) é o número de instâncias que você precisa executar além do permitido pelo limite atual. A calculadora adiciona o limite atual à Instance count (Contagem de instâncias) para obter um novo limite.

A captura de tela a seguir mostra a calculadora de limite de vCPU.

Instance type	Instance count	vCPU count	Current limit	New limit
m5.2xlarge	32	256 vCPUs	2,016 vCPUs	2,272 vCPUs
c5.4xlarge	16	256 vCPUs	2,016 vCPUs	2,272 vCPUs
f1.16xlarge	2	128 vCPUs	176 vCPUs	304 vCPUs

Instance limit name	Current limit	vCPUs needed	New limit	Options
All Standard (A, C, D, H, I, M, R, T, Z) instances	2,016 vCPUs	512 vCPUs	2,528 vCPUs	Request limit increase
All F instances	176 vCPUs	128 vCPUs	304 vCPUs	Request limit increase

Você pode ver e usar os seguintes controles e informações:

- Instance type (Tipo de instância) – Os tipos de instância que você adiciona à calculadora de limite de vCPU.
- Instance count (Número de instâncias) – o número de instâncias necessárias para o tipo de instância selecionado.
- vCPU count (Número de vCPUs) – o número de vCPUs que corresponde ao Instance count (Número de instâncias).
- Current limit (Limite atual) – seu limite atual para o tipo de limite ao qual o tipo de instância pertence. O limite se aplica a todos os tipos de instância do mesmo tipo de limite. Por exemplo: na captura de tela anterior, o limite atual para `m5.2xlarge` e `c5.4xlarge` é de 1.920 vCPUs, que é o limite para todos os tipos de instância que pertencem ao limite de instâncias All Standard.
- New limit (Novo limite) – o novo limite, em número de vCPUs, que é calculado ao adicionar vCPU count (Número de vCPUs) e Current limit (Limite atual).
- X – Selecione X para remover a linha.
- Add instance type (Adicionar tipo de instância) – Selecione Add instance type (Adicionar tipo de instância) para adicionar outro tipo de instância à calculadora.
- Limits calculation (Cálculo de limites) – exibe o limite atual, as vCPUs necessárias e o novo limite para os tipos de limite.
 - Instance limit name (Nome do limite de instância) – o tipo de limite para os tipos de instância selecionados.
 - Current limit (Limite atual) – O limite atual para o tipo de limite.
 - vCPUs needed (vCPUs necessárias) – o número de vCPUs que corresponde ao número de instâncias especificadas na Instance count (Contagem de instâncias). Para o tipo de limite de instâncias All Standard, as vCPUs necessárias são calculadas adicionando os valores do vCPU count (Número de vCPUs) para todos os tipos de instância deste tipo de limite.

- New limit (Novo limite) – o novo limite é calculado adicionando Current limit (Limite atual) e vCPUs needed (vCPUs necessárias).
- Options (Opções) – Selecione Request limit increase (Solicitar aumento de limite) para solicitar um aumento de limite para o tipo de limite correspondente.

Como calcular o número de vCPUs necessárias

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione uma região.
3. No navegador esquerdo, selecione Limits (Limites).
4. Selecione Calculate vCPU limit (Calcular limite de vCPU).
5. Selecione Add instance type (Adicionar tipo de instância), escolha o tipo de instância necessária e especifique o número necessário de instâncias. Para adicionar mais tipos de instância, selecione novamente Add instance type (Adicionar tipo de instância).
6. Veja Limits calculation (Cálculo de limites) para obter o novo limite necessário.
7. Quando terminar de usar a calculadora, selecione Close (Fechar).

Solicitar um aumento de limite de

Você pode solicitar um aumento de limite para cada tipo de limite de instância sob demanda na [página de limites](#) ou na calculadora de limite de vCPU no console do Amazon EC2. Preencha os campos obrigatórios no [formulário](#) de aumento de limite da AWS SupportCentral com seu caso de uso. Para Primary Instance Type (Tipo de instância principal), selecione o tipo de limite que corresponde ao Instance limit name (Nome de limite de instância) na calculadora de limite de vCPU. Para obter o novo valor de limite, use o valor que aparece na coluna New limit (Novo limite) na calculadora de limite de vCPU. Para obter mais informações sobre como solicitar um aumento de limite, consulte [Cotas de serviço do Amazon EC2 \(p. 1567\)](#).

Monitorar limites e uso de instância sob demanda

Você pode visualizar e gerenciar seus limites do instância sob demanda usando o seguinte:

- A [página Limites](#) no console do Amazon EC2
- A [página Cotas de serviços](#) do Amazon EC2 no console de Cotas de serviços
- O `get-service-quota` da AWS CLI
- A [página Limites de serviço](#) no console do AWS Trusted Advisor

Para obter mais informações, consulte [Cotas de serviço do Amazon EC2 \(p. 1567\)](#) no Amazon EC2 User Guide for Linux Instances (Manual do usuário do Amazon EC2 para instâncias do Linux), [Viewing a Service Quota \(Visualizar uma cota de serviço\)](#) no Service Quotas User Guide (Manual do usuário do Service Quotas) e [AWS Trusted Advisor](#).

Com a integração de métricas do Amazon CloudWatch, é possível monitorar o uso do EC2 em comparação aos limites. Também é possível configurar alarmes para alertar quando estiver chegando próximo ao limite. Para obter mais informações, consulte [Usar alarmes do Amazon CloudWatch](#) no Guia do usuário de cotas de serviço.

Consulte os preços das instâncias sob demanda

Você pode usar a API do serviço de lista de preços ou a API da lista de preços da AWS para consultar os preços de instâncias sob demanda. Para obter mais informações, consulte [Using the AWS Price List API \(Usar a API da lista de preços da AWS\)](#) no AWS Billing and Cost Management User Guide (Manual do usuário do AWS Billing and Cost Management).

Reserved Instances

As instâncias reservadas proporcionam economia significativa em seus custos do Amazon EC2 em comparação com os preços de instâncias sob demanda. As instâncias reservadas não são instâncias físicas, mas um desconto na fatura aplicado na sua conta pelo uso de instâncias sob demanda. Essas Instâncias on-demand devem corresponder a determinados atributos, como o tipo de instância e a região, para que você possa aproveitar os benefícios do desconto de faturamento.

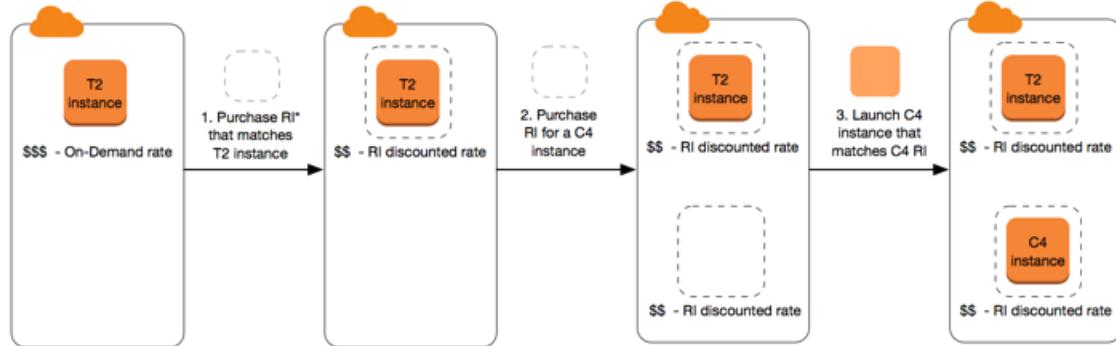
O Savings Plans também oferece economias significativas nos custos do Amazon EC2 comparado à definição de preço de instância sob demanda. Com o Savings Plans, você se compromete com uma quantidade consistente de uso, medida em USD por hora. Isso oferece a flexibilidade de usar as configurações de instância que melhor atendam às suas necessidades e continuar economizando dinheiro, em vez de se comprometer com uma configuração de instância específica. Para obter mais informações, consulte o [Guia do usuário do AWS Savings Plans](#).

Tópicos de Instâncias reservadas

- [Visão geral da Instância reservada \(p. 259\)](#)
- [Principais variáveis que determinam a definição de preço da Instância reservada \(p. 260\)](#)
- [Limites de Instância reservada \(p. 261\)](#)
- [Instâncias reservadas regionais e zonais \(escopo\) \(p. 262\)](#)
- [Tipos de Instâncias reservadas \(classes de oferta\) \(p. 263\)](#)
- [Como as Instâncias reservadas são aplicadas \(p. 263\)](#)
- [Use as suas Instâncias reservadas \(p. 269\)](#)
- [Como você é cobrado \(p. 269\)](#)
- [Comprar Instâncias reservadas \(p. 274\)](#)
- [Vender no Marketplace de instâncias reservadas \(p. 283\)](#)
- [Modificar a Instâncias reservadas \(p. 289\)](#)
- [Trocar Instâncias reservadas conversíveis \(p. 293\)](#)

Visão geral da Instância reservada

O diagrama a seguir mostra uma visão geral básica da compra e do uso das Instâncias reservadas.



Neste cenário, você tem uma instância sob demanda (T2) em execução na sua conta, pela qual paga atualmente as tarifas sob demanda. Você compra uma Instância reservada que corresponde aos atributos da instância em execução, e o benefício do faturamento é aplicado imediatamente. Em seguida, você compra uma Instância reservada para uma instância C4. Você não tem nenhuma instância em execução

na conta que corresponda aos atributos dessa Instância reservada. Na etapa final, execute uma instância que corresponda aos atributos da Instância reservada C4 para que o benefício do faturamento seja aplicado imediatamente.

Principais variáveis que determinam a definição de preço da Instância reservada

A definição de preço de Instância reservada é determinada pelas principais variáveis a seguir.

Atributos da instância

Uma instância reservada tem quatro atributos de instância que determinam seu preço.

- Tipo de instância: Por exemplo, `m4.large`. Isso é composto pela família de instâncias (por exemplo, `m4`) e pelo tamanho da instância (por exemplo, `large`).
- Região: a região na qual a Instância reservada é comprada.
- Locação: Se sua instância é executada em hardware compartilhado (padrão) ou com grupo de usuários único (dedicado). Para obter mais informações, consulte [Dedicated Instances \(p. 383\)](#).
- Plataforma: O sistema operacional; por exemplo, Windows ou Linux/Unix. Para obter mais informações, consulte [Escolher uma plataforma \(p. 274\)](#).

Compromisso com o período de vigência

Você pode comprar uma Instância reservada para um compromisso de um ou três anos, sendo que há um grande desconto para o compromisso de três anos.

- Um ano: o compromisso de um ano é definido como 31536000 segundos (365 dias).
- Três anos: o compromisso de três anos é definido como 94608000 segundos (1095 dias).

As Instâncias reservadas não são renovadas automaticamente; quando elas expiram, você pode continuar usando a instância do EC2 sem interrupções, mas serão cobradas taxas sob demanda. No exemplo acima, quando as Instâncias reservadas que cobrem as instâncias T2 e C4 expirarem, você voltará a pagar as taxas sob demanda até encerrar as instâncias ou comprar novas Instâncias reservadas que correspondam aos atributos de instância.

Opções de pagamento

As seguintes opções de pagamento estão disponíveis para Instâncias reservadas:

- Pagamento adiantado integral: o pagamento integral é feito no início do período de vigência, sem outros custos ou cobranças por hora incorridos pelo restante do período, independentemente das horas usadas.
- Adiantamento parcial: uma parte do custo deve ser paga adiantada, e as horas restantes do período de vigência são faturadas em uma taxa por hora com desconto, independentemente de a Instância reservada estar ou não sendo usada.
- Sem pagamento adiantado: é cobrada a tarifa por hora com desconto para cada hora do período de vigência, independentemente de a Instância reservada estar ou não sendo usada. Nenhum pagamento adiantado é necessário.

Note

As Instâncias reservadas sem pagamento adiantado têm como base uma obrigação contratual de pagamento mensal pelo período de vigência da reserva. Por esse motivo, é necessário ter

um histórico de faturamento de sucesso para que seja possível comprar Instâncias reservadas sem pagamento adiantado.

Em linhas gerais, você pode economizar mais ao fazer um pagamento adiantado maior pelas Instâncias reservadas. Você também pode encontrar instâncias reservadas oferecidas por vendedores terceirizados a preços menores e períodos de vigência mais curtos no Marketplace de instâncias reservadas. Para obter mais informações, consulte [Vender no Marketplace de instâncias reservadas \(p. 283\)](#).

Classe de oferta

Se sua computação precisar de uma mudança, você talvez consiga modificar ou trocar a Instância reservada, dependendo da classe de oferta.

- Padrão: fornece o desconto mais significativo, mas só pode ser modificada. As Instâncias reservadas não podem ser alteradas.
- Conversível: fornece um desconto menor que o das Instâncias reservadas padrão, mas pode ser trocada por outra Instância reservada conversível com atributos de instância diferentes. As Instâncias reservadas conversíveis também podem ser modificadas.

Para obter mais informações, consulte [Tipos de Instâncias reservadas \(classes de oferta\) \(p. 263\)](#).

Após adquirir uma Instância reservada, você não poderá cancelar a compra. Contudo, você poderá [modificar \(p. 289\)](#), [trocar \(p. 293\)](#) ou [vender \(p. 283\)](#) a Instância reservada caso suas necessidades mudem.

Para obter mais informações, consulte a [página Definição de preço de instâncias reservadas do Amazon EC2](#).

Limites de Instância reservada

Há um limite para o número de Instâncias reservadas que você pode comprar por mês. Para cada região você pode comprar 20 Instâncias reservadas [regionais \(p. 264\)](#) por mês além de um adicional de 20 Instâncias reservadas [zonais \(p. 264\)](#) por mês para cada zona de disponibilidade.

Por exemplo, em uma região com três zonas de disponibilidade, o limite é 80 Instâncias reservadas por mês: 20 Instâncias reservadas regionais para a região mais 20 Instâncias reservadas zonais para cada uma das três zonas de disponibilidade ($20 \times 3 = 60$).

Um regional Instância reservada aplica um desconto para um instância sob demanda em execução. O instância sob demanda padrão é 20. Não é possível exceder o limite de execução do instância sob demanda, comprando regional Instâncias reservadas. Por exemplo, se você já tem 20 Instâncias on-demand em execução e você adquiri 20 regional Instâncias reservadas, essas 20 regional Instâncias reservadas serão usadas para aplicar desconto nas 20 Instâncias on-demand em execução. Se você compra mais regional Instâncias reservadas, não será possível iniciar mais instâncias porque alcançou seu limite do instância sob demanda.

Antes de comprar Instâncias reservadas regionais, verifique se o limite de instância sob demanda corresponde ou excede o número de Instâncias reservadas regionais que você pretende ter. Se necessário, solicite um aumento de seu limite de instância sob demanda antes de comprar mais Instâncias reservadas regionais.

Uma zonal Instância reservada—a Instância reservada que é comprada para uma Zona de disponibilidade — específica, e que fornece reserva de capacidade, bem como um desconto. Você pode exceder o limite de execução do instância sob demanda, comprando zonal Instâncias reservadas. Por exemplo, se você já tem 20 Instâncias on-demand em execução e você adquiri 20 zonal Instâncias reservadas, você

pode iniciar mais 20 Instâncias on-demand que correspondam às especificações de sua zonal Instâncias reservadas, dando a você um total de 40 instâncias em execução.

O console do Amazon EC2 fornece informações de limite. Para obter mais informações, consulte [Visualizar os limites atuais \(p. 1567\)](#).

Instâncias reservadas regionais e zonais (escopo)

Ao comprar uma Instância reservada, você determina o escopo da Instância reservada. O escopo pode ser regional ou zonal.

- Regional: quando você compra uma Instância reservada para uma região, ela é chamada de Instância reservada regional.
- Zonal: quando você compra uma Instância reservada para uma zona de disponibilidade específica, ela é chamada de Instância reservada zonal.

O escopo não afeta o preço. Você paga o mesmo preço por um Instância reservada regional ou zonal.

Para obter mais informações sobre Instância reserva da definição de preço, consulte [Principais variáveis que determinam a definição de preço da Instância reservada \(p. 260\)](#) and [Definição de preço de instâncias reservadas do Amazon EC2](#).

Diferenças entre Instâncias reservadas regionais e zonais

A tabela a seguir destaca algumas das principais diferenças entre regionais Instâncias reservadas e zonais Instâncias reservadas:

	Instâncias reservadas regionais	Instâncias reservadas zonais
Capacidade de reservar capacidade	Uma Instância reservada regional não reserva capacidade.	Uma Instância reservada zonal reserva capacidade na zona de disponibilidade especificada.
Flexibilidade da zona de disponibilidade	O desconto da Instância reservada se aplica ao uso da instância em qualquer zona de disponibilidade na região especificada.	Sem flexibilidade da zona de disponibilidade — o desconto da Instância reservada se aplica ao uso da instância somente na zona de disponibilidade especificada.
Flexibilidade de tamanho da instância	O desconto da Instância reservada se aplica ao uso da instância na família de instâncias, independentemente do tamanho. Compatível somente com Instâncias reservadas de Linux/Unix da Amazon com locação padrão. Para obter mais informações, consulte Flexibilidade de tamanho da instância determinada pelo fator de normalização (p. 264) .	Sem flexibilidade de tamanho da instância — o desconto da Instância reservada se aplica ao uso da instância somente para o tamanho e o tipo de instância especificados.
Enfileiramento de uma compra	Você pode enfileirar compras para instâncias reservadas regionais.	Você não pode enfileirar compras para instâncias reservadas zonais.

Para obter mais informações e exemplos, consulte [Como as Instâncias reservadas são aplicadas \(p. 263\)](#).

Tipos de Instâncias reservadas (classes de oferta)

A classe de oferta de uma Instância reservada é padrão ou conversível. Uma Instância reservada padrão oferece um desconto mais significativo do que uma Instância reservada conversível, mas você não pode trocar uma Instância reservada padrão. Você pode trocar Instâncias reservadas conversíveis. Você pode modificar Instâncias reservadas padrão e conversíveis.

A configuração de uma Instância reservada compreende um único tipo de instância, plataforma, escopo e locação ao longo de um termo. Se suas necessidades de computação mudarem, talvez seja possível modificar ou trocar a sua Instância reservada.

Diferenças entre Instâncias reservadas padrão e conversível

A seguir estão as diferenças entre as classes de oferta da Instâncias reservadas padrão e conversível.

	Instância reservada padrão	Convertible Reserved Instance
Modificando Instâncias reservadas	Alguns atributos podem ser modificados. Para obter mais informações, consulte Modificar a Instâncias reservadas (p. 289) .	Alguns atributos podem ser modificados. Para obter mais informações, consulte Modificar a Instâncias reservadas (p. 289) .
Trocar Instâncias reservadas	Não pode ser trocada.	Pode ser trocada durante o período de vigência por outra Instância reservada convertível com novos atributos, incluindo a família de instâncias, o tipo de instância, a plataforma, o escopo ou a locação. Para obter mais informações, consulte Trocar Instâncias reservadas conversíveis (p. 293) .
Vender no Marketplace de instâncias reservadas	Pode ser vendida no Marketplace de instâncias reservadas.	Não pode ser vendida no Marketplace de instâncias reservadas.
Comprar no Marketplace de instâncias reservadas	Pode ser comprada no Marketplace de instâncias reservadas.	Não pode ser comprada no Marketplace de instâncias reservadas.

Como as Instâncias reservadas são aplicadas

Se você tiver adquirido uma Instância reservada e já tiver uma instância em execução que corresponda às especificações da Instância reservada, o benefício de faturamento será aplicado imediatamente. Você não tem de reiniciar suas instâncias. Se você não tiver uma instância em execução qualificada, execute uma instância atendendo aos mesmos critérios especificados para a Instância reservada. Para obter mais informações, consulte [Use as suas Instâncias reservadas \(p. 269\)](#).

As Instâncias reservadas se aplicam ao uso da mesma forma, independentemente do tipo de oferta (padrão ou conversível), e são aplicadas automaticamente às Instâncias on-demand em execução com atributos correspondentes.

Como as Instâncias reservadas zonais são aplicadas

As Instâncias reservadas atribuídas a uma zona de disponibilidade específica oferecem à Instância reservada descontos pelo uso de instância correspondente nessa zona de disponibilidade. Por exemplo, se você tiver adquirido duas c4.xlarge padrão Linux/Unix Instâncias reservadas de locação padrão na zona de disponibilidade us-east-1a, até duas instâncias Linux/Unix c4.xlarge de locação padrão em execução na zona de disponibilidade us-east-1a poderão se beneficiar com o desconto da Instância reservada. Os atributos (locação, plataforma, zona de disponibilidade, tipo de instância e tamanho de instância) das instâncias em execução devem corresponder aos atributos das Instâncias reservadas.

Como as Instâncias reservadas regionais são aplicadas

As Instâncias reservadas regionais são compradas para uma região e fornecem flexibilidade de zona de disponibilidade. O desconto da Instância reservada se aplica ao uso da instância em qualquer zona de disponibilidade nessa região.

As Instâncias reservadas regionais também fornecem flexibilidade de tamanho da instância quando o desconto da Instância reservada se aplica ao uso da instância na família de instâncias, independentemente do tamanho.

Limites para a flexibilidade de tamanho da instância

A flexibilidade de tamanho da instância não se aplica às seguintes Instâncias reservadas:

- Instâncias reservadas compradas para uma zona de disponibilidade específica (Instâncias reservadas zonal)
- Instâncias reservadas com locação dedicada
- Instâncias reservadas para Windows Server, Windows Server com SQL Standard, Windows Server com SQL Server Enterprise, Windows Server com SQL Server Web, RHEL e SUSE Linux Enterprise Server
- Instâncias reservadas para instâncias do G4dn

Flexibilidade de tamanho da instância determinada pelo fator de normalização

A flexibilidade de tamanho da instância é determinada pelo fator de normalização do tamanho da instância. O desconto se aplica total ou parcialmente às instâncias em execução da mesma família de instâncias, dependendo do tamanho da instância da reserva, em qualquer zona de disponibilidade na região. Os únicos atributos que devem ser correspondentes são a locação, a plataforma e a família de instâncias.

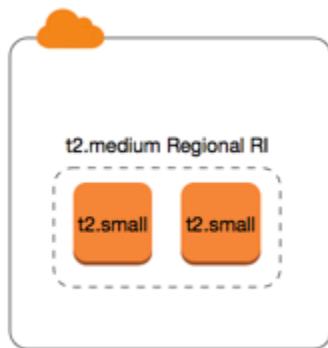
A flexibilidade do tamanho da instância é aplicada do menor para o maior tamanho de instância na família de instâncias com base no fator de normalização.

A tabela a seguir descreve os diferentes tipos em uma família de instâncias e o fator de normalização correspondente por hora. Essa escala é usada para aplicar a taxa de desconto de Instâncias reservadas ao uso normalizado da família de instâncias.

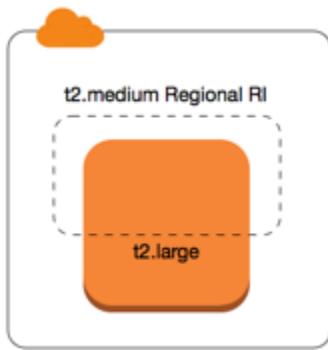
Tamanho da instância	Fator de normalização
nano	0.25
micro	0,5
small	1
medium	2
large	4

Tamanho da instância	Fator de normalização
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
56xlarge	448
112xlarge	896

Por exemplo, uma instância `t2.medium` tem um fator de normalização de 2. Se você tiver adquirido uma Instância reservada `t2.medium` de Linux/Unix da Amazon de locação padrão na US East (N. Virginia) e tiver duas instâncias `t2.small` em execução em sua conta nessa região, o benefício de faturamento será aplicado integralmente às duas instâncias.



Ou, se você tiver uma instância `t2.large` em execução em sua conta na região US East (N. Virginia) o benefício de faturamento será aplicado a 50% do uso da instância.



O fator de normalização é aplicado também ao modificar Instâncias reservadas. Para obter mais informações, consulte [Modificar a Instâncias reservadas \(p. 289\)](#).

Fator de normalização para instâncias bare metal

A flexibilidade de tamanho da instância também se aplica a instâncias bare metal na família de instâncias. Se você tem Instâncias reservadas regionais de Linux/Unix da Amazon com locação compartilhada em instâncias bare metal, é possível se beneficiar das economias de Instância reservada na mesma família de instâncias. O inverso também é verdadeiro: se você tem Instâncias reservadas regionais de Linux/Unix da Amazon com locação compartilhada em instâncias na mesma família que uma instância bare metal, é possível se beneficiar das economias de Instância reservada na instância bare metal.

O tamanho da instância `metal` não tem um único fator de normalização. Uma instância bare metal tem o mesmo fator de normalização que o tamanho de instância virtualizada equivalente dentro da mesma família de instâncias. Por exemplo, uma instância `i3.metal` tem o mesmo fator de normalização que uma instância `i3.16xlarge`.

Tamanho da instância	Fator de normalização
<code>m5zn.metal</code> <code>z1d.metal</code>	96
<code>i3.metal</code>	128
<code>c5n.metal</code>	144
<code>c5.metal</code> <code>c5d.metal</code> <code>i3en.metal</code> <code>m5.metal</code> <code>m5d.metal</code> <code>m5dn.metal</code> <code>m5n.metal</code> <code>r5.metal</code> <code>r5b.metal</code> <code>r5d.metal</code> <code>r5dn.metal</code> <code>r5n.metal</code>	192
<code>u-* .metal</code>	896

Por exemplo, uma instância `i3.metal` tem um fator de normalização de 128. Se você comprar uma Instância reservada `i3.metal` de Linux/Unix da Amazon de locação padrão na US East (N. Virginia), o benefício de faturamento poderá ser aplicado da seguinte maneira:

- Se você tem uma instância `i3.16xlarge` em execução em sua conta nessa região, o benefício de faturamento é aplicado integralmente à instância `i3.16xlarge` (fator de normalização da `i3.16xlarge` = 128).
- Ou, se você tem duas instâncias `i3.8xlarge` em execução em sua conta nessa região, o benefício de faturamento é aplicado integralmente a ambas as instâncias `i3.8xlarge` (fator de normalização da `i3.8xlarge` = 64).
- Ou, se você tem quatro instâncias `i3.4xlarge` em execução em sua conta nessa região, o benefício de faturamento é aplicado integralmente a todas as quatro instâncias `i3.4xlarge` (fator de normalização da `i3.4xlarge` = 32).

O inverso também é verdadeiro. Por exemplo, se você comprar duas Instâncias reservadas *i3.8xlarge* de Linux/Unix da Amazon de locação padrão na US East (N. Virginia) e tiver uma instância *i3.metal* em execução nessa região, o benefício de faturamento será aplicado integralmente à instância *i3.metal*.

Exemplos de aplicação da Instâncias reservadas

Os cenários a seguir abrangem as maneiras como as Instâncias reservadas são aplicadas.

Example Cenário 1: Instâncias reservadas em uma única conta

Você está executando as seguintes Instâncias on-demand na conta A:

- 4 x instâncias do Linux *m3.large* de locação padrão na zona de disponibilidade us-east-1a
- 2 x instâncias do Amazon Linux *m4.xlarge* de locação padrão na zona de disponibilidade us-east-1b
- 1 x instâncias do Amazon Linux *c4.xlarge* de locação padrão na zona de disponibilidade us-east-1c

Você adquire as seguintes Instâncias reservadas na conta A:

- 4 Instâncias reservadas Linux *m3.large* de locação padrão na zona de disponibilidade us-east-1a (a capacidade é reservada)
- 4 x Instâncias reservadas *m4.large* de locação padrão do Amazon Linux na região us-east-1
- 1 x Instâncias reservadas *c4.large* de locação padrão do Amazon Linux na região us-east-1

Os benefícios da Instância reservada são aplicados da seguinte maneira:

- O desconto e a reserva de capacidade das quatro Instâncias reservadas *m3.large* zonais são usados pelas quatro instâncias *m3.large*, pois os atributos (tamanho da instância, região, plataforma, locação) entre elas são correspondentes.
- As *m4.large* Instâncias reservadas regionais fornecem flexibilidade de zona de disponibilidade e de tamanho de instância, pois são Instâncias reservadas Amazon Linux regionais com locação padrão.

m4.large é equivalente a 4 unidades normalizadas/hora.

Você adquiriu quatro Instâncias reservadas *m4.large* regionais e, no total, elas equivalem a 16 unidades normalizadas/hora (4x4). A conta A tem duas instâncias *m4.xlarge* em execução, equivalente a 16 unidades normalizadas/hora (2x8). Nesse caso, as quatro Instâncias reservadas *m4.large* regionais fornecem o benefício de faturamento a uma hora inteira de uso das duas instâncias *m4.xlarge*.

- A Instância reservada *c4.large* regional em us-east-1 fornece flexibilidade de zona de disponibilidade e de tamanho da instância, pois é uma Instância reservada Amazon Linux regional com locação padrão e se aplica à instância *c4.xlarge*. Uma instância *c4.large* é equivalente a 4 unidades normalizadas/hora e a uma *c4.xlarge* é equivalente a 8 unidades normalizadas/hora.

Nesse caso, a *c4.large* Instância reservada regional fornece benefício parcial para uso de *c4.xlarge*. Isso ocorre porque a Instância reservada *c4.large* equivale a 4 unidades normalizadas/hora de uso, mas a instância *c4.xlarge* requer 8 unidades normalizadas/hora. Portanto, o desconto de faturamento da Instância reservada *c4.large* aplica-se a 50% do uso de *c4.xlarge*. O uso *c4.xlarge* restante é cobrado na tarifa sob demanda.

Example Cenário 2: Instâncias reservadas regionais em contas vinculadas

As Instâncias reservadas são aplicadas primeiro ao uso na conta de compra, seguida pelo uso de qualificação em qualquer outra conta da organização. Para obter mais informações, consulte [Instâncias reservadas e faturamento consolidado \(p. 271\)](#). Para Instâncias reservadas regionais que oferecem flexibilidade de tamanho de instância, o benefício é aplicado do menor para o maior tamanho de instância na família de instâncias.

Você está executando a seguinte Instâncias on-demand na conta A (a conta de compra):

- 2 x instâncias do Linux **m4.xlarge** de locação padrão na zona de disponibilidade us-east-1a
- 1 x instâncias do Linux **m4.2xlarge** de locação padrão na zona de disponibilidade us-east-1b
- 2 x instâncias do Linux **c4.xlarge** de locação padrão na zona de disponibilidade us-east-1a
- 1 x instâncias do Linux **c4.2xlarge** de locação padrão na zona de disponibilidade us-east-1b

Outro cliente está executando as seguintes Instâncias on-demand na conta B — uma conta vinculada:

- 2 x instâncias do Linux **m4.xlarge** de locação padrão na zona de disponibilidade us-east-1a

Você adquire as seguintes Instâncias reservadas regionais na conta A:

- 4 x Instâncias reservadas **m4.xlarge** de locação padrão do Linux na região us-east-1
- 2 x Instâncias reservadas **c4.xlarge** de locação padrão do Linux na região us-east-1

Os benefícios da Instância reservada regional são aplicados da seguinte maneira:

- O desconto das quatro Instâncias reservadas **m4.xlarge** é usado pelas duas instâncias **m4.xlarge** e pela única instância **m4.2xlarge** na conta A (conta de compra). Todas as três instâncias têm atributos correspondentes (locação, plataforma região e família de instâncias). O desconto é aplicado às instâncias da conta de compra (conta A) primeiro, mesmo que a conta B (conta vinculada) tenha duas **m4.xlarge** que também correspondam às Instâncias reservadas. Não há reserva de capacidade, pois as Instâncias reservadas são regionais Instâncias reservadas.
- O desconto das duas Instâncias reservadas **c4.xlarge** se aplica às duas instâncias **c4.xlarge**, porque eles são um tamanho de instância menor que a instância **c4.2xlarge**. Não há reserva de capacidade, pois as Instâncias reservadas são regionais Instâncias reservadas.

Example Cenário 3: Instâncias reservadas zonais em uma conta vinculada

Geralmente, as Instâncias reservadas pertencentes a uma conta são aplicadas primeiro ao uso nessa conta. Contudo, se houver Instâncias reservadas qualificadas e não utilizadas para uma zona de disponibilidade específica (Instâncias reservadas zonais) em outras contas da organização, elas serão aplicadas à conta antes das Instâncias reservadas regionais pertencentes à conta. Isso é feito para garantir a utilização máxima da Instância reservada e uma fatura menor. Para fins de faturamento, todas as contas da organização são tratadas como se fossem uma só. O exemplo a seguir pode ajudar a explicar isso.

Você está executando a seguinte instância sob demanda na conta A (a conta de compra):

- 1 x instância do Linux **m4.xlarge** de locação padrão na zona de disponibilidade us-east-1a

Um cliente está executando a seguinte instância sob demanda na conta vinculada B:

- 1 x instância do Linux **m4.xlarge** de locação padrão na zona de disponibilidade us-east-1b

Você adquire as seguintes Instâncias reservadas regionais na conta A:

- 1 x Instância reservada **m4.xlarge** de locação padrão do Linux na região us-east-1

Um cliente também compra as seguintes Instâncias reservadas de zona na conta C vinculada:

- 1 **m4.xlarge** Linux Instâncias reservadas de locação padrão na zona de disponibilidade us-east-1a

Os benefícios da Instância reservada são aplicados da seguinte maneira:

- O desconto da Instância reservada m4.xlarge de zona pertencente à conta C é aplicado ao uso de m4.xlarge na conta A.
- O desconto da Instância reservada m4.xlarge regional pertencente à conta A é aplicado ao uso de m4.xlarge na conta B.
- Se a Instância reservada regional pertencente à conta A tiver sido aplicada primeiro ao uso na conta A, a Instância reservada de zona pertencente à conta C permanecerá não utilizada, e o uso na conta B será cobrado nas taxas sob demanda.

Para obter mais informações, consulte [Instâncias reservadas no relatório do Billing and Cost Management](#).

Use as suas Instâncias reservadas

As Instâncias reservadas são aplicadas automaticamente às Instâncias on-demand em execução, desde que as especificações sejam correspondentes. Se você não tiver nenhuma Instância on-demand que corresponda às especificações de sua Instância reservada, a Instância reservada não será utilizada até que você execute uma instância com as especificações necessárias.

Se você estiver executando uma instância para aproveitar o benefício de faturamento de uma Instância reservada, especifique as informações a seguir durante a execução:

- Plataforma: escolha uma imagem de máquina da Amazon (AMI) que corresponda à plataforma (descrição de produtos) da Instância reservada. Por exemplo, se você tiver especificado Linux/UNIX, pode executar uma instância a partir de um Amazon Linux AMI ou Ubuntu AMI.
- Tipo de instância: especifique o mesmo tipo de instância de sua Instância reservada; por exemplo, t2.large.
- Zona de disponibilidade: se você tiver adquirido uma Instância reservada para uma zona de disponibilidade específica, deverá executar a instância na mesma zona de disponibilidade. Se você tiver adquirido uma Instância reservada regional, poderá executar a instância em qualquer zona de disponibilidade.
- Locação: a locação da sua instância deve corresponder à locação da Instância reservada; por exemplo, dedicated ou shared. Para obter mais informações, consulte [Dedicated Instances \(p. 383\)](#).

Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#). Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte [Como as Instâncias reservadas são aplicadas \(p. 263\)](#).

Você pode usar o Amazon EC2 Auto Scaling ou outros serviços da AWS para executar as instâncias sob demanda que usam os benefícios da instância reservada. Para mais informações, consulte o [Guia do usuário do Amazon EC2 Auto Scaling](#).

Como você é cobrado

Todas as Instâncias reservadas fornecem um desconto em comparação à definição de preço sob demanda. Com as Instâncias reservadas, você paga por todo o período de vigência, e não pelo uso real. Você pode optar por pagar pela Instância reservada adiantado, parcialmente adiantado ou mensalmente, dependendo da [opção de pagamento \(p. 260\)](#) especificada para a Instância reservada.

Quando as Instâncias reservadas expirarem, serão cobradas taxas sob demanda pelo uso da instância do EC2. É possível colocar uma Instância reservada em uma fila para compra por até três anos de maneira antecipada. Isso pode ajudar a garantir que você tenha cobertura ininterrupta. Para obter mais informações, consulte [Enfileirar sua compra \(p. 275\)](#).

O nível gratuito da AWS está disponível para novas contas da AWS. Se você estiver usando o nível gratuito da AWS para executar instâncias do Amazon EC2 e adquirir uma instância reservada, será

cobrado de acordo com as diretrizes padrão de definição de preço. Para obter informações, consulte [Nível gratuito da AWS](#).

Tópicos

- [Faturamento do uso \(p. 270\)](#)
- [Visualizar sua fatura \(p. 271\)](#)
- [Instâncias reservadas e faturamento consolidado \(p. 271\)](#)
- [Níveis de definição de preço com desconto da Instância reservada \(p. 272\)](#)

Faturamento do uso

As Instâncias reservadas são cobradas a cada hora fechada durante o período de vigência selecionado, independentemente de uma instância estar sendo executada ou não. Cada hora fechada começa na hora (zero minutos e zero segundos após a hora) de um relógio padrão de 24 horas. Por exemplo, 1:00:00 a 1:59:59 é uma hora fechada. Para obter mais informações sobre os estados da instância, consulte [Ciclo de vida da instância \(p. 412\)](#).

Um benefício do faturamento de Instância reservada pode ser aplicado a uma instância em execução com base em uma taxa por segundo.

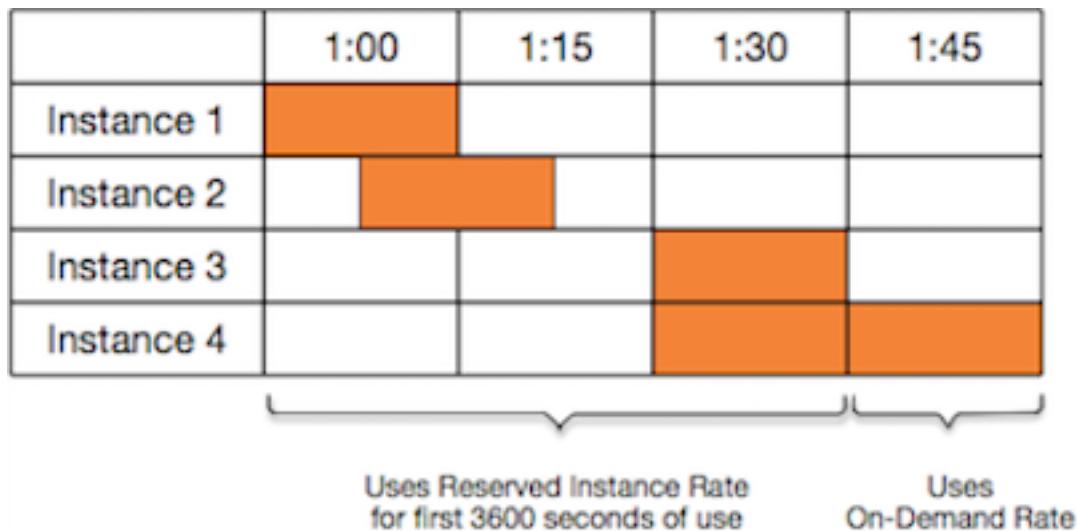
Um dos benefícios de faturamento da Instância reservada pode ser aplicado a um máximo de 3600 segundos (uma hora) de uso de instância por hora fechada. Você pode executar várias instâncias simultaneamente, mas só pode receber o benefício do desconto de Instância reservada por um total de 3600 segundos por hora. O uso de instância que ultrapassar 3600 segundos em uma hora será faturado com base na taxa sob demanda.

Por exemplo, se você adquirir uma Instância reservada `m4.xlarge` e executar quatro instâncias `m4.xlarge` simultaneamente por uma hora, uma instância será cobrada em uma hora de uso de Instância reservada, enquanto as outras três instâncias serão cobradas em três horas de uso sob demanda.

Contudo, se você adquirir uma Instância reservada `m4.xlarge` e executar quatro instâncias `m4.xlarge` por 15 minutos (900 segundos) cada uma dentro da mesma hora, o tempo total de execução das instâncias será uma hora, o que resultará em uma hora de uso de Instância reservada e 0 hora de uso sob demanda.

	1:00	1:15	1:30	1:45
Instance 1				
Instance 2				
Instance 3				
Instance 4				

Se várias instâncias qualificadas estiverem sendo executadas simultaneamente, o benefício de faturamento de Instância reservada será aplicado a todas as instâncias ao mesmo tempo até um máximo de 3600 segundos em uma hora. Depois disso, serão cobradas taxas sob demanda.



O Cost Explorer no console do [Billing and Cost Management](#) permite que você analise as economias com base nas Instâncias on-demand em execução. As [perguntas frequentes sobre Instâncias reservadas](#) incluem um exemplo de um cálculo de valor de tabela.

Se você fechar sua conta na AWS, o faturamento sob demanda dos seus recursos será interrompido. Contudo, se você tiver Instâncias reservadas na conta, continuará recebendo a fatura delas até que elas expirem.

Visualizar sua fatura

Você encontrará mais informações sobre as cobranças e as taxas da sua conta ao visualizar o console do [AWS Billing and Cost Management](#).

- O Painel exibe um resumo de gastos da sua conta.
- Na página Bills (Faturas), em Details (Detalhes), expanda a seção Elastic Compute Cloud e a região para obter informações de faturamento sobre suas Instâncias reservadas.

Você pode visualizar as cobranças online ou baixar um arquivo CSV.

Você também pode monitorar a utilização da instância reservada usando o Relatório de uso e de custo da AWS. Para obter mais informações, consulte [Reserved Instances \(Instâncias reservadas\)](#) em Relatório de uso e de custo no AWS Billing and Cost Management User Guide (Manual do usuário do AWS Billing and Cost Management).

Instâncias reservadas e faturamento consolidado

Os benefícios da definição de preços das Instâncias reservadas são compartilhados quando a conta que faz a compra é parte de um conjunto de contas faturadas sob uma conta pagante de faturamento consolidado. O uso da instância em todas as contas-membro é agregada na conta pagante todos os meses. Em geral, isso é útil para empresas em que há equipes ou grupos funcionais diferentes; dessa forma, a lógica usual da Instância reservada é aplicada para calcular a conta. Para obter mais informações, consulte [Faturamento consolidado para o AWS Organizations](#).

Se você fechar a conta que comprou a Instância reservada, a conta pagante será cobrada pela Instância reservada até que a instância reservada expire. Depois que a conta encerrada for excluída permanentemente em 90 dias, as contas de membro não se beneficiarão mais do desconto de faturamento da instância reservada.

Níveis de definição de preço com desconto da Instância reservada

Se sua conta se qualificar para uma camada de preços com desconto, ela receberá automaticamente descontos nas taxas de uso de instância e com pagamento adiantado nas compras de Instância reservada que você fizer nessa camada, desse ponto em diante. Para se qualificar para um desconto, o valor de tabela das Instâncias reservadas na região deverá ser de 500.000 USD ou mais.

As seguintes regras se aplicam:

- As camadas de preços e descontos relacionados aplicam-se somente às compras das Amazon EC2 padrão do Instâncias reservadas.
- As camadas de preços não se aplicam às Instâncias reservadas para Windows com SQL Server Standard, SQL Server Web e SQL Server Enterprise.
- As camadas de preços não se aplicam às Instâncias reservadas para Linux com SQL Server Standard, SQL Server Web e SQL Server Enterprise.
- Os descontos do nível de preços aplicam-se somente às compras feitas pela AWS. Eles não se aplicam a compras de Instâncias reservadas de terceiros.
- As camadas de preços com desconto atualmente não são aplicáveis a compras de Instância reservada convertível.

Tópicos

- [Calcular descontos de preço de Instância reservada \(p. 272\)](#)
- [Comprar com nível de desconto \(p. 273\)](#)
- [Cruzamento de níveis de definição de preço \(p. 273\)](#)
- [Faturamento consolidado para níveis de definição de preço \(p. 274\)](#)

Calcular descontos de preço de Instância reservada

Você pode determinar a camada da definição de preço de sua conta ao calcular o valor de tabela de todas as Instâncias reservadas em uma região. Multiplique o preço recorrente por hora de cada reserva pelo número total de horas do período de vigência e adicione o preço adiantado sem desconto (conhecido também como preço fixo) no momento da compra. Como o valor de tabela se no preço sem desconto (público), ele não será afetado se você se qualificar para um desconto por volume ou se o preço cair depois de você comprar suas Instâncias reservadas.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Por exemplo, para uma t2.small Instância reservada com adiantamento parcial de 1 ano, supõe-se que o preço inicial seja 60,00 USD e a taxa por hora seja 0,007 USD. Isso fornece um valor de tabela de 121,32 USD.

```
121.32 = 60.00 + (0.007 * 8760)
```

New console

Para ver os valores de preço fixo das Instâncias reservadas usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias reservadas.
3. Para exibir a coluna Upfront price (Preço inicial), escolha o ícone de configurações () no canto superior direito, ative Upfront price(Preço inicial) e escolha Confirm (Confirmar).

Old console

Para ver os valores de preço fixo das Instâncias reservadas usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias reservadas.
3. Para exibir a coluna Upfront price (Preço inicial), escolha o ícone de configurações () no canto superior direito, selecione Upfront price (Preço inicial) e escolha Close (Fechar).

Para ver os valores de preço fixo das Instâncias reservadas usando a linha de comando

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (AWS Tools for Windows PowerShell)
- [DescribeReservedInstances](#) (API do Amazon EC2)

Comprar com nível de desconto

Quando você comprar Instâncias reservadas, o Amazon EC2 aplicará automaticamente todos os descontos à parte da sua compra que estiver dentro do nível de preço com desconto. Você não precisará fazer nada diferente e poderá comprar as Instâncias reservadas usando qualquer ferramenta do Amazon EC2. Para obter mais informações, consulte [Comprar Instâncias reservadas \(p. 274\)](#).

Depois que o valor de tabela das Instâncias reservadas ativas em uma região ultrapassar um nível de definição de preço com desconto, qualquer compra futura de Instâncias reservadas nessa região será cobrada com uma taxa com desconto. Se com uma única compra de Instâncias reservadas em uma região você ultrapassar o limite de uma camada com desconto, a parte da compra que estiver acima do limite de preço será cobrada com a taxa com desconto. Para obter mais informações sobre os IDs de Instância reservada temporária criados durante o processo de compra, consulte [Cruzamento de níveis de definição de preço \(p. 273\)](#).

Se o valor de tabela ficar abaixo do ponto de preço desse nível de definição de preço com desconto — por exemplo, se algumas das Instâncias reservadas expirarem — as futuras compras de Instâncias reservadas na região não receberão desconto. Contudo, você continua a receber o desconto aplicado em todas as Instâncias reservadas originalmente compradas no nível de preço com desconto.

Estes são os quatro cenários possíveis durante a compra de Instâncias reservadas:

- Sem desconto — sua compra em uma região ainda está abaixo do limite para desconto.
- Desconto parcial — sua compra em uma região ultrapassa o limite do primeiro nível de desconto. Nenhum desconto é aplicado a uma ou mais reservas e a taxa com desconto é aplicada nas reservas restantes.
- Desconto total — sua compra inteira em uma região cai em um nível de desconto e recebe o desconto apropriado.
- Duas taxas com desconto — sua compra em uma região ultrapassa um nível inferior de desconto para um nível superior de desconto. Serão cobradas duas taxas diferentes: uma ou mais reservas na taxa desconto inferior e as reservas restantes com a taxa desconto maior.

Cruzamento de níveis de definição de preço

Se sua compra cruzar um nível de preços com desconto, você verá múltiplas entradas para essa compra: uma para a parte da compra cobrada em preço normal e outra para essa a parte da compra cobrada na taxa de desconto aplicável.

O serviço Instância reservada gera vários IDs de Instância reservada porque sua compra passou de um nível sem desconto ou de um nível com desconto para outro. Há um ID para cada conjunto de reservas em um nível. Portanto, o ID retornado pelo comando de compra da CLI ou pela ação da API é diferente do ID real das novas Instâncias reservadas.

Faturamento consolidado para níveis de definição de preço

Uma conta de faturamento consolidado agrupa o valor de tabela das contas-membro em uma região. Quando o valor de tabela de todas as Instâncias reservadas ativas para a conta de faturamento consolidado atingir uma camada de preços com desconto, todas as Instâncias reservadas compradas depois desse ponto por qualquer membro da conta de faturamento consolidado serão cobradas com o desconto (desde que o valor de tabela para essa conta consolidada fique acima de limite de camada de preços com desconto). Para obter mais informações, consulte [Instâncias reservadas e faturamento consolidado \(p. 271\)](#).

Comprar Instâncias reservadas

Para comprar uma instância reservada, pesquise por ofertas de instância reservada na AWS e em vendedores terceirizados, ajustando os parâmetros de pesquisa até encontrar a correspondência exata que está procurando.

Quando você procurar Instâncias reservadas para comprar, receberá um orçamento do custo das ofertas apresentadas. Ao dar continuidade à compra, a AWS colocará automaticamente um preço-limite sobre o preço de compra. O custo total das suas Instâncias reservadas não excederá o valor orçado.

Se o preço aumentar ou mudar por algum motivo, a compra não será concluída. Se, no momento da compra, houver ofertas semelhantes à sua escolha, mas por um preço menor, a AWS venderá as ofertas a preços mais baixos.

Antes de confirmar sua compra, analise os detalhes da Instância reservada que planeja comprar e verifique se todos os parâmetros são precisos. Após adquirir uma instância reservada (do vendedor terceirizado no Marketplace de instâncias reservadas ou da AWS), você não poderá cancelar sua compra.

Note

Para comprar e modificar instâncias reservadas, certifique-se de que sua conta de usuário do IAM tenha as permissões apropriadas, como a capacidade de descrever zonas de disponibilidade.

Para obter mais informações, consulte [Example Policies for Working With the AWS CLI or an AWS SDK \(Exemplos de políticas para trabalhar com a AWS CLI ou um AWS SDK\)](#) e [Example Policies for Working in the Amazon EC2 Console](#).

Tópicos

- [Escolher uma plataforma \(p. 274\)](#)
- [Enfileirar sua compra \(p. 275\)](#)
- [Comprar Instâncias reservadas padrão \(p. 275\)](#)
- [Comprar Instâncias reservadas conversíveis \(p. 278\)](#)
- [Comprar do Marketplace da Instância reservada \(p. 280\)](#)
- [Como exibir o Instâncias reservadas \(p. 281\)](#)
- [Como cancelar uma compra colocada na fila \(p. 281\)](#)
- [Renovar uma Instância reservada \(p. 282\)](#)

Escolher uma plataforma

O Amazon EC2 é compatível com as seguintes plataformas Windows para Instâncias reservadas:

- Windows
- Windows com SQL Server Standard

- Windows com SQL Server Web
- Windows com SQL Server Enterprise

Quando adquire uma Instância reservada, você deve escolher uma oferta para uma plataforma que represente o sistema operacional da sua instância.

- Para Windows com SQL Standard, Windows com SQL Server Enterprise e Windows com SQL Server Web, você deve escolher ofertas específicas para essas plataformas.
- Para todas as demais versões do Windows, escolha uma oferta para a plataforma Windows.

Important

Se você planeja comprar uma instância reservada para aplicar a uma instância sob demanda iniciado a partir de uma AMI do AWS Marketplace , primeiro verifique o campo `PlatformDetails` da AMI. O campo `PlatformDetails` indica qual Instância reservada comprar. Os detalhes da plataforma da AMI devem corresponder à plataforma da Instância reservada, caso contrário, a Instância reservada não será aplicado ao instância sob demanda. Para obter informações sobre como visualizar os detalhes da plataforma da AMI, consulte [Noções básicas sobre as informações de faturamento da AMI \(p. 140\)](#).

Para obter informações sobre as plataformas compatíveis com Linux, consulte [Como escolher uma plataforma](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Enfileirar sua compra

Por padrão, quando você compra uma Instância reservada, a compra é feita imediatamente. Se preferir, você poderá colocar as compras na fila para uma data e hora futura. Por exemplo, é possível colocar uma compra na fila para o momento próximo da expiração de uma Instância reservada existente. Isso pode ajudar a garantir que você tenha cobertura ininterrupta.

É possível colocar compras na fila para uma Instâncias reservadas regional, mas não para uma Instâncias reservadas zonal ou uma Instâncias reservadas de outros vendedores. É possível colocar uma compra na fila por até três anos de maneira antecipada. Na data e hora programadas, a compra será executada usando a forma de pagamento padrão. Após o pagamento ser feito com êxito, os benefícios de faturamento serão aplicados.

É possível visualizar as compras colocadas na fila no console do Amazon EC2. O status de uma compra na fila é `queued` (na fila). É possível cancelar uma compra na fila a qualquer momento antes da hora programada. Para obter mais detalhes, consulte [Como cancelar uma compra colocada na fila \(p. 281\)](#).

Comprar Instâncias reservadas padrão

Você pode comprar as Instâncias reservadas padrão em uma zona de disponibilidade específica e obter uma reserva de capacidade. Como alternativa, você pode abandonar a reserva de capacidade e comprar uma Instância reservada padrão regional;

New console

Para comprar Instâncias reservadas padrão usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instances reservadas (Comprar Instâncias reservadas).
3. Para Offering class (Classe da oferta), escolha Standard (Padrão) para exibir as Instâncias reservadas padrão.
4. Para comprar uma reserva de capacidade, escolha Only show offerings that reserve capacity (Mostrar apenas ofertas que reservam capacidade) no canto superior direito da tela de compra.

Quando você ativa essa configuração, o campo Availability Zone (Zona de disponibilidade) é exibido.

Para comprar um Instância reservada regional, desative essa configuração. Quando você desativa essa configuração, o campo Availability Zone (Zona de disponibilidade) desaparece.

5. Selecione outras configurações conforme necessário e escolha Search (Pesquisar).
6. Para cada Instância reservada que você deseja comprar, insira a quantidade e escolha Add to cart (Adicionar ao carrinho).

Para comprar uma instância reservada padrão no Marketplace de instâncias reservadas, procure por 3rd Party (terceiros) na coluna Seller (Vendedor) dos resultados de pesquisa. A coluna Termo exibe os termos não padrão. Para obter mais informações, consulte [Comprar do Marketplace da Instância reservada \(p. 280\)](#).

7. Para ver um resumo das Instâncias reservadas selecionadas, escolha View cart (Visualizar carrinho).
8. Se Order on (Pedir em) for Now (Agora), a compra será concluída imediatamente após você escolher Order all (Pedir tudo). Para colocar uma compra na fila, selecione Now (Agora) e selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.
9. Para concluir o pedido, selecione Order all (Pedir tudo).

Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.

10. Escolha Close (Fechar).

O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de Payment-pending para Active. Quando a Instância reservada for Active, ela estará pronta para ser usada.

Note

Se o status for para Retired, a AWS pode não ter recebido seu pagamento.

Old console

Para comprar Instâncias reservadas padrão usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instances reservadas (Comprar Instâncias reservadas).
3. Para Offering class (Classe da oferta), escolha Standard (Padrão) para exibir as Instâncias reservadas padrão.
4. Para comprar uma reserva de capacidade, escolha Mostrar apenas ofertas que reservam capacidade no canto superior direito da tela de compra. Para comprar uma Instância reservada regional, deixe a caixa de seleção desmarcada.
5. Selecione outras configurações conforme o necessário e escolha Pesquisar.

Para comprar uma instância reservada padrão no Marketplace de instâncias reservadas, procure por 3rd Party (terceiros) na coluna Seller (Vendedor) dos resultados de pesquisa. A coluna Termo exibe os termos não padrão.

6. Para cada Instância reservada que você deseja comprar, insira a quantidade e escolha Add to Cart (Adicionar ao carrinho).
7. Para ver um resumo das Instâncias reservadas selecionadas, escolha View cart (Visualizar carrinho).

8. Se Order On (Pedir em) for Now (Agora), a compra será concluída imediatamente. Para colocar uma compra na fila, selecione Now (Agora) e selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.
9. Para concluir o pedido, selecione Order (Fazer pedido).

Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.

10. Escolha Close (Fechar).

O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de payment-pending para active. Quando a Instância reservada for active, ela estará pronta para ser usada.

Note

Se o status for para retired, a AWS pode não ter recebido seu pagamento.

Para comprar uma instância reservada padrão usando a AWS CLI

1. Localize as Instâncias reservadas disponíveis usando o comando `describe-reserved-instances-offerings`. Especifique standard para o parâmetro --offering-class apresentar somente Instâncias reservadas padrão. Você pode aplicar parâmetros adicionais para restringir os resultados. Por exemplo, se você quiser comprar uma Instância reservada regional t2.large com uma locação padrão para Linux/UNIX durante um período de vigência de somente 1 ano:

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=duration,Values=31536000 Name=scope,Values=Region
```

Para localizar as instâncias reservadas somente no Marketplace de instâncias reservadas, use o filtro `marketplace` e não especifique uma duração na solicitação, pois o período de vigência pode ser mais curto que o período de 1 ou 3 anos.

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class standard \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=marketplace,Values=true
```

Quando encontrar uma Instância reservada que atenda às suas necessidades, anote o ID da oferta. Por exemplo:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Use o comando `purchase-reserved-instances-offering` para comprar sua Instância reservada. Você deve especificar o ID de oferta da Instância reservada obtido na etapa anterior e o número de instâncias da reserva.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
```

```
--instance-count 1
```

Por padrão, a compra será concluída imediatamente. Se preferir, para colocar a compra na fila, adicione o parâmetro a seguir à chamada anterior.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Use o comando [describe-reserved-instances](#) para obter o status da Instância reservada.

```
aws ec2 describe-reserved-instances
```

Como alternativa, use os seguintes comandos do AWS Tools for Windows PowerShell:

- [Get-EC2ReservedInstancesOffering](#)
- [New-EC2ReservedInstance](#)
- [Get-EC2ReservedInstance](#)

Após concluir a compra, se você já tiver uma instância em execução que corresponda às especificações da Instância reservada, o benefício de faturamento será aplicado imediatamente. Você não tem de reiniciar suas instâncias. Se você não tiver uma instância em execução adequada, execute uma instância atendendo aos mesmos critérios especificados para a Instância reservada. Para obter mais informações, consulte [Use as suas Instâncias reservadas \(p. 269\)](#).

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte [Como as Instâncias reservadas são aplicadas \(p. 263\)](#).

Comprar Instâncias reservadas conversíveis

Você pode comprar Instâncias reservadas conversíveis em uma zona de disponibilidade específica e obter uma reserva de capacidade. Como alternativa, você pode abandonar a reserva de capacidade e comprar uma Instância reservada convertível regional.

New console

Para comprar Instâncias reservadas conversíveis usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instances reserved (Comprar Instâncias reservadas).
3. Em Offering class (Classe da oferta), escolha Convertible (Conversível) para exibir as Instâncias reservadas conversíveis.
4. Para comprar uma reserva de capacidade, escolha Only show offerings that reserve capacity (Mostrar apenas ofertas que reservam capacidade) no canto superior direito da tela de compra. Quando você ativa essa configuração, o campo Availability Zone (Zona de disponibilidade) é exibido.

Para comprar um Instância reservada regional, desative essa configuração. Quando você desativa essa configuração, o campo Availability Zone (Zona de disponibilidade) desaparece.

5. Selecione outras configurações conforme o necessário e escolha Pesquisar.
6. Para cada Instância reservada convertível que você deseja comprar, insira a quantidade e escolha Add to cart (Adicionar ao carrinho).
7. Para ver um resumo da sua seleção, escolha View cart (Visualizar carrinho).
8. Se Order on (Pedir em) for Now (Agora), a compra será concluída imediatamente após você escolher Order all (Pedir tudo). Para colocar uma compra na fila, selecione Now (Agora) e

selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.

9. Para concluir o pedido, selecione Order all (Pedir tudo).

Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.

10. Escolha Close (Fechar).

O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de `Payment-pending` para `Active`. Quando a Instância reservada for `Active`, ela estará pronta para ser usada.

Note

Se o status for para `Retired`, a AWS pode não ter recebido seu pagamento.

Old console

Para comprar Instâncias reservadas conversíveis usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reserved Instances (Instâncias reservadas) e Purchase Instâncias reservadas (Comprar Instâncias reservadas).
3. Em Offering class (Classe da oferta), escolha Convertible (Conversível) para exibir as Instâncias reservadas conversíveis.
4. Para comprar uma reserva de capacidade, escolha Mostrar apenas ofertas que reservam capacidade no canto superior direito da tela de compra. Para comprar uma Instância reservada regional, deixe a caixa de seleção desmarcada.
5. Selecione outras configurações conforme o necessário e escolha Pesquisar.
6. Para cada Instância reservada convertível que você deseja comprar, insira a quantidade e escolha Add to Cart (Adicionar ao carrinho).
7. Para ver um resumo da sua seleção, escolha View cart (Visualizar carrinho).
8. Se Order On (Pedir em) for Now (Agora), a compra será concluída imediatamente. Para colocar uma compra na fila, selecione Now (Agora) e selecione uma data. É possível selecionar uma data diferente para cada oferta elegível no carrinho. A compra é enfileirada até às 00:00 UTC da data selecionada.
9. Para concluir o pedido, selecione Order (Fazer pedido).

Se, no momento de fazer o pedido, houver ofertas semelhantes à sua escolha, mas com um preço menor, a AWS venderá as ofertas pelo preço mais baixo.

10. Escolha Close (Fechar).

O status do seu pedido é listado na coluna State (Estado). Quando o pedido estiver concluído, veja o valor Estado mudar de `payment-pending` para `active`. Quando a Instância reservada for `active`, ela estará pronta para ser usada.

Note

Se o status for para `retired`, a AWS pode não ter recebido seu pagamento.

Para comprar uma instância reservada conversível usando a AWS CLI

1. Localize as Instâncias reservadas disponíveis usando o comando `describe-reserved-instances-offerings`. Especifique `convertible` para o parâmetro `--offering-class` apresentar somente

Instâncias reservadas conversíveis. Você pode aplicar parâmetros adicionais para estreitar seus resultados; por exemplo, se você quiser comprar uma Instância reservada regional `t2.large` com uma locação padrão para Linux/UNIX:

```
aws ec2 describe-reserved-instances-offerings \
    --instance-type t2.large \
    --offering-class convertible \
    --product-description "Linux/UNIX" \
    --instance-tenancy default \
    --filters Name=scope,Values=Region
```

Quando encontrar uma Instância reservada que atenda às suas necessidades, anote o ID da oferta. Por exemplo:

```
"ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
```

2. Use o comando `purchase-reserved-instances-offering` para comprar sua Instância reservada. Você deve especificar o ID de oferta da Instância reservada obtido na etapa anterior e o número de instâncias da reserva.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

Por padrão, a compra será concluída imediatamente. Se preferir, para colocar a compra na fila, adicione o parâmetro a seguir à chamada anterior.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Use o comando `describe-reserved-instances` para obter o status da Instância reservada.

```
aws ec2 describe-reserved-instances
```

Como alternativa, use os seguintes comandos do AWS Tools for Windows PowerShell:

- [Get-EC2ReservedInstancesOffering](#)
- [New-EC2ReservedInstance](#)
- [Get-EC2ReservedInstance](#)

Se você já tiver uma instância em execução que corresponda às especificações da Instância reservada, o benefício de faturamento será imediatamente aplicado. Você não tem de reiniciar suas instâncias. Se você não tiver uma instância em execução adequada, execute uma instância atendendo aos mesmos critérios especificados para a Instância reservada. Para obter mais informações, consulte [Use as suas Instâncias reservadas \(p. 269\)](#).

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte [Como as Instâncias reservadas são aplicadas \(p. 263\)](#).

Comprar do Marketplace da Instância reservada

Você pode adquirir instâncias reservadas de vendedores terceiros que tenham instâncias reservadas de que não precisam mais do Marketplace de instâncias reservadas. Você pode fazer isso usando o console do Amazon EC2 ou a ferramenta de linha de comando. O processo é semelhante à compra de instâncias reservadas da AWS. Para obter mais informações, consulte [Comprar Instâncias reservadas padrão \(p. 275\)](#).

Existem poucas diferenças entre instâncias reservadas adquiridas no Marketplace de instâncias reservadas e instâncias reservadas adquiridas diretamente da AWS:

- Período de vigência: as instâncias reservadas que você compra de terceiros têm menos que um período de vigência padrão completo restante. Os períodos de vigência completos da AWS são de um ano ou três anos.
- Preço adiantado: as instâncias reservadas de terceiros podem ser vendidas em preços adiantados diferentes. As taxas de uso ou recorrentes são as mesmas que as taxas definidas quando as instâncias reservadas foram adquiridas originalmente da AWS.
- Tipos de instâncias reservadas: somente instâncias reservadas padrão do Amazon EC2 podem ser adquiridas no Marketplace de instâncias reservadas. Instâncias reservadas conversíveis, Amazon RDS e Amazon ElastiCache não estão disponíveis para compra no Marketplace de instâncias reservadas.

Informações básicas sobre você são compartilhadas com o vendedor – por exemplo, seu código postal e as informações do país.

Essas informações permitem que os vendedores calculem os impostos de transação necessários que precisam remeter ao governo (como impostos sobre vendas ou imposto sobre valor agregado) e são fornecidas na forma de um relatório de desembolso. Em raras circunstâncias, a AWS pode ter de fornecer ao vendedor seu endereço de e-mail, de forma que possam entrar em contato com você sobre as perguntas relacionadas à venda (por exemplo, dúvidas sobre impostos).

Por motivos semelhantes, a AWS compartilha a razão social do vendedor na fatura de compra do comprador. Se você precisar de mais informações sobre o vendedor para fins de impostos ou algo relacionado, entre em contato com o [AWS Support](#).

Como exibir o Instâncias reservadas

Você pode visualizar as Instâncias reservadas adquiridas usando o console do Amazon EC2 ou uma ferramenta de linha de comando.

Para visualizar as Instâncias reservadas no console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias reservadas.
3. Seus Instâncias reservadas em fila, ativos e retirados estarão listados. A coluna Estado exibe o estado.
4. Se você for um vendedor no Marketplace de instâncias reservadas, a aba My Listings (Minhas ofertas) exibirá o status de uma reserva listada no [Marketplace de instâncias reservadas \(p. 283\)](#). Para obter mais informações, consulte [Estados de listagem da Instância reservada \(p. 287\)](#).

Para visualizar as Instâncias reservadas usando a linha de comando

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (Tools for Windows PowerShell)

Como cancelar uma compra colocada na fila

É possível colocar uma compra na fila por até três anos de maneira antecipada. É possível cancelar uma compra na fila a qualquer momento antes da hora programada.

New console

Como cancelar uma compra colocada na fila

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione uma ou mais Instâncias reservadas.
4. Selecione Actions (Ações), Delete Queued Reserved Instances (Excluir instâncias reservadas na fila).
5. Quando a confirmação for solicitada, insira Delete (Excluir) e escolha Close (Fechar).

Old console

Como cancelar uma compra colocada na fila

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione uma ou mais Instâncias reservadas.
4. Selecione Actions (Ações), Delete Queued Reserved Instances (Excluir instâncias reservadas na fila).
5. Quando a confirmação for solicitada, escolha Yes, Delete (Sim, excluir).

Como cancelar uma compra na fila usando a linha de comando

- [delete-queued-reserved-instances](#) (AWS CLI)
- [Remove-EC2QueuedReservedInstance](#) (Tools for Windows PowerShell)

Renovar uma Instância reservada

Você pode renovar uma Instância reservada antes que ela esteja programada para expirar. Renovar uma Instância reservada coloca a compra de uma Instância reservada na fila com a mesma configuração até que a Instância reservada atual expire.

New console

Como renovar uma Instância reservada usando uma compra na fila

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione uma ou mais Instâncias reservadas.
4. Escolha Actions (Ações), Renew Reserved Instances (Renovar instâncias reservadas).
5. Para concluir o pedido, escolha Order all (Pedir tudo) e, em seguida, Close (Fechar).

Old console

Como renovar uma Instância reservada usando uma compra na fila

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione uma ou mais Instâncias reservadas.
4. Escolha Actions (Ações), Renew Reserved Instances (Renovar instâncias reservadas).
5. Para concluir o pedido, selecione Order (Fazer pedido).

Vender no Marketplace de instâncias reservadas

O Marketplace de instâncias reservadas é uma plataforma compatível com a venda padrão de instâncias reservadas padrão não utilizadas de clientes da AWS e de terceiros, que variam em termos de duração e opções de preço. Por exemplo, você pode desejar vender instâncias reservadas depois de mover instâncias para uma nova região da AWS, alterar para um novo tipo de instância, concluir projetos antes da expiração do prazo, quando suas necessidades de negócio mudarem ou tiver capacidade desnecessária.

Assim que você oferecer suas instâncias reservadas no Marketplace de instâncias reservadas, elas serão disponibilizadas para que possíveis compradores as encontrem. Todas as Instâncias reservadas são agrupadas de acordo com a duração do período de vigência restante e do preço por hora.

Para atender à solicitação de um comprador, a AWS primeiro vende a instância reservada com o menor preço inicial no agrupamento especificado. Então, a AWS vende a instância reservada com o menor preço até que o pedido inteiro do comprador seja cumprido. A AWS então, processa as transações e transfere a propriedade das instâncias reservadas ao comprador.

Você manterá a propriedade da Instância reservada até ela ser vendida. Após venda, você abre mão da reserva de capacidade e das taxas recorrentes com desconto. Se você continuar a usar sua instância, a AWS cobrará de você o preço sob demanda, a partir do momento em que sua instância reservada foi vendida.

Se você quiser vender suas instâncias reservadas não utilizadas no Marketplace de instâncias reservadas, deverá atender a determinados critérios de elegibilidade.

Para obter mais informações sobre como comprar instâncias reservadas no Marketplace de instâncias reservadas, consulte [Comprar do Marketplace da Instância reservada \(p. 280\)](#).

Tópicos

- [Restrições e limitações \(p. 283\)](#)
- [Registre-se como vendedor \(p. 284\)](#)
- [Conta de banco para desembolso \(p. 284\)](#)
- [Informações fiscais \(p. 285\)](#)
- [Precificar suas Instâncias reservadas \(p. 286\)](#)
- [Liste as suas Instâncias reservadas \(p. 286\)](#)
- [Estados de listagem da Instância reservada \(p. 287\)](#)
- [Ciclo de vida de uma lista \(p. 287\)](#)
- [Depois que a Instância reservada é vendida \(p. 288\)](#)
- [Recebimentos \(p. 288\)](#)
- [Informações compartilhadas com o comprador \(p. 289\)](#)

Restrições e limitações

Antes que você possa vender suas reservas não utilizadas, é necessário registrar-se como vendedor no Marketplace de instâncias reservadas. Para obter mais informações, consulte [Registre-se como vendedor \(p. 284\)](#).

As seguintes limitações e restrições são aplicáveis na venda da Instâncias reservadas:

- Somente as instâncias reservadas padrão do Amazon EC2 podem ser vendidas no Marketplace de instâncias reservadas. Instâncias reservadas conversíveis do Amazon EC2 não podem ser vendidas. Instâncias reservadas para outros produtos da AWS, como o Amazon RDS e o Amazon ElastiCache, não podem ser vendidas.
- Deve haver pelo menos um mês restante no período de vigência da Instância reservada padrão.
- Não é possível vender uma Instância reservada standard em uma região que é [desativada por padrão](#).

- O preço mínimo permitido no Marketplace de instâncias reservadas é 0,00 USD.
- Você pode vender instâncias reservadas sem adiantamento, com adiantamento parcial ou adiantamento integral no Marketplace de instâncias reservadas. Se houver um pagamento adiantado em uma instância reservada, ela só pode ser vendida após a AWS receber o pagamento adiantado e a reserva estiver ativa (se você for o proprietário) por pelo menos 30 dias.
- Você não pode modificar diretamente sua oferta no Marketplace de instâncias reservadas. No entanto, você pode alterar sua lista primeiro cancelando-a e depois criando outra lista com os parâmetros novos. Para obter mais informações, consulte [Precificar suas Instâncias reservadas \(p. 286\)](#). Você também pode modificar as Instâncias reservadas antes de listá-las. Para obter mais informações, consulte [Modificar a Instâncias reservadas \(p. 289\)](#).
- Para listar uma instância reservada regional no marketplace, é necessário modificar o escopo para zonal, pois não é possível vender instâncias reservadas regionais pelo console.
- A AWS cobra uma taxa de serviço de 12% do preço inicial total de cada instância reservada padrão que você vender no Marketplace de instâncias reservadas. O preço inicial é aquele que o vendedor está cobrando pela Instância reservada padrão;.
- Quando você se registra como vendedor, o banco especificado deve ter um endereço nos EUA. Para obter mais informações, consulte [Requisitos adicionais do vendedor para produtos pagos](#) no Guia do vendedor do AWS Marketplace .
- Os clientes do Amazon Internet Services Private Limited (AISPL) não podem vender instâncias reservadas no Marketplace de instâncias reservadas, mesmo que tenham uma conta bancária nos EUA. Para obter mais informações, consulte [Quais são as diferenças entre as contas da AWS e as contas da AISPL?](#)

Registre-se como vendedor

Note

Somente o usuário raiz da conta da AWS pode registrar uma conta como vendedor.

Para vender no Marketplace de instâncias reservadas, você deve se registrar como vendedor. Durante o registro, você fornecerá as seguintes informações:

- Informações bancárias: a AWS deve ter suas informações bancárias para desembolsar os fundos recolhidos da venda das suas reservas. O banco que você especificar deverá ter um endereço nos EUA. Para obter mais informações, consulte [Conta de banco para desembolso \(p. 284\)](#).
- Informação sobre impostos — todos os vendedores precisam concluir uma entrevista sobre informações de impostos para determinar qualquer obrigação de declaração de impostos necessária. Para obter mais informações, consulte [Informações fiscais \(p. 285\)](#).

Após a AWS receber o registro preenchido do vendedor, você receber um e-mail confirmado seu registro e informando que você pode começar a vender no Marketplace de instâncias reservadas.

Conta de banco para desembolso

A AWS deve ter suas informações bancárias para distribuir os fundos recolhidos quando você vende sua instância reservada. O banco que você especificar deverá ter um endereço nos EUA. Para obter mais informações, consulte [Requisitos adicionais do vendedor para produtos pagos](#) no Guia do vendedor do AWS Marketplace .

Para registrar uma conta de banco padrão para desembolsos

1. Abra a página [Reserved Instance Marketplace Seller Registration \(Registro do vendedor do Marketplace de instâncias reservadas\)](#) e faça login usando as credenciais da AWS.
2. Na página Gerenciar conta bancária, forneça as informações a seguir sobre o banco para receber o pagamento:

- Nome do titular da conta
- Número de roteamento
- Número da conta
- Tipo de conta bancária

Note

Se você estiver usando uma conta bancária corporativa, será solicitado que envie as informações sobre a conta bancária via fax (1-206-765-3424).

Após o registro, a conta bancária fornecida é definida como padrão, ficando pendente a verificação com o banco. Pode demorar até duas semanas para verificar uma conta bancária nova, e durante esse tempo você não poderá receber desembolsos. Para uma conta estabelecida, geralmente leva cerca de dois dias para os desembolsos serem concluídos.

Para alterar a conta de banco padrão para o desembolso

1. Na página [Reserved Instance Marketplace Seller Registration \(Registro do vendedor do Marketplace de instâncias reservadas\)](#), faça login na conta que você usou ao se registrar.
2. Na página Gerenciar conta bancária, adicione uma conta bancária nova ou modifique a conta bancária padrão conforme necessário.

Informações fiscais

A venda de Instâncias reservadas pode estar sujeita a um imposto baseado em transação, como imposto sobre vendas ou imposto sobre valor agregado. Você deve verificar com os departamentos fiscal, jurídico, financeiro ou contábil da sua empresa para determinar a aplicabilidade dos impostos de transação. Você é responsável para coletar e enviar impostos de transação para a devida autoridade fiscal.

Como parte do processo de registro do vendedor, é necessário completar uma entrevista sobre impostos no [Portal de registro do vendedor](#). O entrevista coleta suas informações sobre impostos e preenche um formulário W-9, W-8BEN ou W-8BEN-E de IRS, que é usado para determinar todas as obrigações de declaração de impostos necessárias.

As informações sobre impostos inseridas como parte da entrevista sobre impostos pode diferir dependendo se você opera como um indivíduo ou como um negócio, e se você ou o seu negócio são ou não uma pessoa ou entidade dos EUA. Enquanto preenche a entrevista fiscal, tenha em mente o seguinte:

- Informações fornecidas pela AWS, inclusive as informações deste tópico, não constituem orientações jurídicas, fiscais ou profissional de alguma outra forma. Para descobrir como os requisitos de relatório da IRS podem afetar seu negócio, ou se você tiver outras dúvidas, entre em contato com seu orientador fiscal, jurídico ou profissional.
- Para atender os requisitos de relatório da IRS da forma mais eficiente possível, responda todas as perguntas e insira todas as informações solicitadas durante a entrevista.
- Verifique suas respostas. Evite erros de ortografia ou inserir números de identificação fiscal incorretos. Eles podem resultar em um formulário de impostos invalidado.

Com base nas respostas da entrevista fiscal e nos limites de declaração de imposto de renda, a Amazon pode registrar o Formulário 1099-K. A Amazon envia uma cópia do Formulário 1099-K em 31 de janeiro, ou antes disso, do ano seguinte ao ano em que sua conta fiscal chegar aos níveis do limite. Por exemplo, se sua conta atingir o limite em 2018, o formulário 1099-K será enviado até 31 de janeiro de 2019.

Para obter mais informações sobre os requisitos da IRS e o Formulário 1099-K, consulte o site da [IRS](#).

Precificar suas Instâncias reservadas

A taxa de adiantamento é a única taxa que você pode especificar para a Instância reservada que está vendendo. A taxa de adiantamento é a taxa única que o comprador paga ao comprar uma Instância reservada.

É importante observar os limites a seguir:

- Você pode vender até 50.000 USD em Instâncias reservadas. Para aumentar esse limite, preencha o formulário de [vendas de Instância reservada do EC2](#).
- Você pode vender até 5.000 Instâncias reservadas. Para aumentar esse limite, preencha o formulário de [vendas de Instância reservada do EC2](#).
- O preço mínimo é 0 USD \$0. O preço mínimo permitido no Marketplace de instâncias reservadas é 0,00 USD.

Você não pode modificar diretamente sua lista. No entanto, você pode alterar sua lista primeiro cancelando-a e depois criando outra lista com os parâmetros novos.

Você pode cancelar sua lista a qualquer momento, desde que ela esteja no estado `active`. Você não poderá cancelar a lista se já houver correspondência ou se ela estiver sendo processada para uma venda. Se houver correspondências em algumas das instâncias da sua lista e você cancelar a lista, somente as instâncias não correspondentes restantes serão removidas.

Como o valor das instâncias reservadas diminui com o tempo, por padrão a AWS pode definir os preços para diminuir em incrementos iguais mês a mês. No entanto, você pode os preços iniciais diferentes com base nas vendas da sua reserva.

Por exemplo, se sua Instância reservada tiver nove meses de prazo restante, você pode especificar a quantidade que aceitaria se um cliente comprar essa Instância reservada com nove meses restantes. É possível definir outro preço com cinco meses restantes, e ainda outro preço com um mês restante.

Liste as suas Instâncias reservadas

Como vendedor registrado, você pode optar por vender uma ou mais de suas Instâncias reservadas. Você pode escolher vender todos eles em uma lista ou em partes. Além disso, você pode listar as Instâncias reservadas com qualquer configuração de tipo de instância, plataforma e escopo.

O console determina um preço sugerido. Ele verifica as ofertas que correspondem à Instância reservada e relaciona a que tiver o preço mais baixo. Caso contrário, ele calcula um preço sugerido com base no custo da Instância reservada pelo tempo restante. Se o valor calculado for menor que 1,01 USD, o preço sugerido será de 1,01 USD.

Se você cancelar sua lista e parte da lista tiver sido vendida, o cancelamento não será eficiente na parte que foi vendida. Somente a parte não vendida da oferta não estará mais disponível no Marketplace de instâncias reservadas.

Para oferecer uma instância reservada no Marketplace de instâncias reservadas usando o AWS Management Console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione as Instâncias reservadas para listar e escolha Actions (Ações) e Sell Instâncias reservadas (Vender Instâncias reservadas).
4. Na página Configurar a lista de Instância reservada, defina o número de instâncias para vender e o preço inicial para o prazo restante nas colunas relevantes. Veja como o valor de sua reserva muda com o restante do período ao selecionar a seta ao lado da coluna Meses restantes.

5. Se você for um usuário avançado e quiser personalizar o preço, poderá inserir valores diferentes nos meses subsequentes. Para retornar à queda de preço linear padrão, escolha Redefinir.
6. Escolha Continuar quando você tiver terminado de configurar sua lista.
7. Confirme os detalhes da sua lista na página Confirmar a lista da sua Instância reservada e, se estiver satisfeito, escolha Listar instância reservada.

Para visualizar suas listas no console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias reservadas.
3. Selecione a Instância reservada listada e escolha a guia My Listings (Minhas ofertas) na parte inferior da página.

Para gerenciar instâncias reservadas no Marketplace de instâncias reservadas usando a AWS CLI

1. Obtenha a lista das suas Instâncias reservadas usando o comando [describe-reserved-instances](#).
2. Anote o ID da Instância reservada que você deseja listar e chame [create-reserved-instances-listing](#). Você deve especificar o ID da Instância reservada, o número de instâncias e a programação de preços.
3. Para visualizar sua lista, use o comando [describe-reserved-instances-listings](#).
4. Para cancelar sua lista, use o comando [cancel-reserved-instances-listings](#).

Estados de listagem da Instância reservada

O Estado da lista na guia Minhas listagens da página de Instâncias reservadas exibe o status atual das listagens:

As informações exibidas por Listing State (Estado da oferta) se referem ao status de sua oferta no Marketplace de instâncias reservadas. Isso é diferente das informações de status exibidas na coluna Estado da página Instâncias reservadas. Essas informações de Estado são sobre sua reserva.

- ativa—A lista está disponível para compra.
- canceled (cancelada): a oferta foi cancelada e não está disponível para compra no Marketplace de instâncias reservadas.
- closed—A Instância reservada não é listada. Uma Instância reservada pode ser closed, pois a venda da listagem foi concluída.

Ciclo de vida de uma lista

Quando todas as instâncias na sua lista forem correspondidas e vendidas, a guia Minhas listas exibirá que a Contagem de instâncias totais corresponde à contagem listada em Vendido. Além disso, não há instâncias Disponíveis deixadas para sua listagem, e o Status é closed.

Quando apenas parte da sua oferta é vendida, a AWS remove as instâncias reservadas na oferta e cria o número de instâncias reservadas igual ao das instâncias reservadas restantes na contagem. Assim, o ID da listagem e a listagem que a representa, que agora tem menos reservas à venda, ainda estão ativas.

Todas as vendas futuras das Instâncias reservadas nessa listagem serão processadas dessa maneira. Quando todas as instâncias reservadas na oferta forem vendidas, a AWS marcará a lista como closed.

Por exemplo, você cria um ID de listagem de Instâncias reservadas 5ec28771-05ff-4b9b-aa31-9e57dexample com uma contagem de 5.

A guia Minhas listas na página do console da Instância reservada exibirá a lista desta forma:

ID de listagem de Instância reservada 5ec28771-05ff-4b9b-aa31-9e57dexample

- Contagem total da reserva = 5
- Vendidas = 0
- Disponíveis = 5
- Status = ativos

Um comprador compra duas das reservas, que deixa uma contagem de três reservas ainda disponíveis para venda. Por conta dessa venda parcial, a AWS cria uma nova reserva com uma contagem de três para representar as reservas restantes que ainda estão à venda.

Sua lista tem a seguinte forma na guia Minha lista:

ID de listagem de Instância reservada 5ec28771-05ff-4b9b-aa31-9e57dexample

- Contagem total da reserva = 5
- Vendidas = 2
- Disponíveis = 3
- Status = ativos

Se você cancelar sua lista e parte da lista já tiver sido vendida, o cancelamento não será eficiente na parte que foi vendida. Somente a parte não vendida da oferta não estará mais disponível no Marketplace de instâncias reservadas.

Depois que a Instância reservada é vendida

Quando a instância reservada for vendida, a AWS enviará uma notificação por e-mail. Cada dia em que houver qualquer tipo de atividade, você receberá uma notificação por e-mail capturando todas as atividades do dia. As atividades podem incluir a criação ou a venda de uma oferta ou o envio de recursos financeiros para sua conta pela AWS.

Como rastrear o status de uma oferta de Instância reservada no console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na página de navegação, escolha Reserved Instances (Instâncias reservadas).
3. Escolha a guia My Listings (Minhas ofertas).

A guia Minhas listas contém o valor de Estado da lista. Ela também contém informações sobre o período, o preço de tabela e um detalhamento de quantas instâncias na lista estão disponíveis, pendentes, vendidas e canceladas.

Você também pode usar o comando [describe-reserved-instances-listings](#) com o filtro apropriado para obter informações sobre suas listas.

Recebimentos

Assim que a AWS receber os valores do comprador, será enviada uma mensagem ao e-mail da conta do proprietário registrado para a instância reservada vendida.

AWSA faz uma transferência bancária via Automated Clearing House (ACH) para sua conta bancária especificada. Normalmente, essa transferência ocorre entre um e três dias após sua Instância reservada ter sido vendida. Os desembolsos ocorrem uma vez por dia. Você receberá um e-mail com o relatório

de desembolso após o recurso financeiro ser liberado. Lembre-se de que você não poderá receber desembolsos até que a AWS tenha recebido verificação do seu banco. Isso pode levar até duas semanas.

A Instância reservada que você vendeu continua aparecendo quando você descreve as Instâncias reservadas.

Você recebe um reembolso em dinheiro pelas instâncias reservadas por meio de uma transferência eletrônica feita diretamente na sua conta bancária. A AWS cobra uma taxa de serviço de 12% do preço inicial total de cada instância reservada vendida no Marketplace de instâncias reservadas.

Informações compartilhadas com o comprador

Quando você vender no Marketplace de instâncias reservadas, a AWS compartilhará o nome legal da empresa no extrato do comprador, de acordo com as normas dos EUA. Além disso, se o comprador acessar o suporte da AWS Support porque precisa entrar em contato com você para obter uma fatura ou por outro motivo relacionado a impostos, a AWS pode precisar fornecer ao comprador no seu endereço de e-mail, de modo que ele possa entrar em contato diretamente com você.

Por motivos semelhantes, as informações de código postal do comprador e do país são fornecidas ao vendedor no relatório de desembolso. Como vendedor, você pode precisar dessas informações para acompanhar todos os impostos de transação necessários que você remeter ao governo (como impostos sobre vendas e impostos de valor agregado).

A AWS não pode oferecer orientações sobre impostos, mas se seu especialistas em impostos determinar que você precisa de informações adicionais específicas, entre em contato com o [Suporte da AWS Support](#).

Modificar a Instâncias reservadas

Quando suas necessidades mudarem, você poderá modificar seu padrão ou Instâncias reservadas conversíveis e continuar usufruindo o benefício de faturamento. Você pode modificar atributos como a zona de disponibilidade e escopo de sua Instância reservada.

Note

Você também pode trocar uma Instância reservada convertível por outra Instância reservada convertível com uma configuração diferente. Para obter mais informações, consulte [Trocando Instâncias reservadas conversíveis \(p. 293\)](#).

Após a modificação, o benefício das Instâncias reservadas será aplicado somente às instâncias que correspondem aos novos parâmetros. Por exemplo, se você alterar a zona de disponibilidade de uma reserva, a reserva de capacidade e os benefícios de preço serão automaticamente aplicados ao uso da instância na nova zona de disponibilidade. Das instâncias que não corresponderem mais aos novos parâmetros, será cobrada a taxa sob demanda, a menos que sua conta tenha outras reservas aplicáveis.

Se sua solicitação da modificação tiver sucesso:

- A reserva modificada entra em vigor imediatamente e o benefício de preço é aplicado às novas instâncias que iniciam na hora da solicitação de modificação. Por exemplo, se você modificar com êxito suas reservas às 9:15PM, o benefício do preço será transferido para sua nova instância às 9:00PM. Você pode obter a data efetiva das Instâncias reservadas modificadas usando o comando [describe-reserved-instances](#).
- A reserva original é desativada. A data final é a data inicial da nova reserva, e a data final da nova reserva é a mesma que a data final da Instância reservada original. Se você modificar uma reserva de três anos com 16 meses sobrando de período de vigência, a reserva modificada resultante será uma reserva de 16 meses com a mesma data final que a original.
- A reserva alterada lista um preço fixo de 0 USD e não o preço fixo da reserva original.
- O preço fixo da reserva modificada não afeta os cálculos da camada de preços com desconto aplicados à sua conta, que são baseados no preço fixo da reserva original.

Se sua solicitação de modificação falhar, as Instâncias reservadas manterão a configuração original e serão imediatamente disponibilizadas para outra solicitação de modificação.

Não há taxas para a modificação e você não receber nenhuma conta ou fatura novas.

Você pode modificar suas reservas quantas vezes quiser, mas não pode alterar nem cancelar uma solicitação de modificação pendente depois da enviá-la. Depois de a modificação ser concluída com sucesso, você pode enviar outra solicitação de modificação para reverter as alterações que fez, se necessário.

Tópicos

- [Requisitos e restrições para modificação \(p. 290\)](#)
- [Enviar solicitações de modificação \(p. 291\)](#)
- [Solucionar problemas de solicitações de modificação \(p. 293\)](#)

Requisitos e restrições para modificação

É possível modificar esses atributos da maneira a seguir.

Atributo modificável	Plataformas compatíveis	Limitações
Alterar as zonas de disponibilidade na mesma região	Linux e Windows	-
Alterar o escopo de zona de disponibilidade para região e vice-versa	Linux e Windows	<p>Se você alterar o escopo de zona de disponibilidade para região, perderá o benefício da reserva de capacidade.</p> <p>Se você alterar o escopo de região para zona de disponibilidade, perderá a flexibilidade da zona de disponibilidade e a flexibilidade de tamanho de instância (se aplicável). Para obter mais informações, consulte Como as Instâncias reservadas são aplicadas (p. 263).</p>
Alterar o tamanho da instância na mesma família de instâncias	Somente Linux/UNIX A flexibilidade do tamanho da instância não está disponível para Instâncias reservadas nas outras plataformas, que incluem Linux com SQL Server Standard, Linux com SQL Server Web, Linux com SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows com SQL Standard, Windows com SQL Server Enterprise e Windows com SQL Server Web.	A reserva deve usar a locação padrão. Para algumas famílias de instâncias não há suporte, pois não há outros tamanhos disponíveis. Para obter mais informações, consulte Suporte para modificação de tamanhos de instância no Guia do usuário do Amazon EC2 para instâncias do Linux.

Atributo modificável	Plataformas compatíveis	Limitações
Alterar a rede do EC2-Classic para a Amazon VPC e vice-versa	Linux e Windows	A plataforma de rede deve estar disponível em sua conta da AWS. Se sua conta da AWS foi criada após 04/12/2013, ela não oferecerá suporte ao EC2-Classic.

Requirements

O Amazon EC2 processará sua solicitação de modificação se houver capacidade suficiente para sua nova configuração (se aplicável) e se as seguintes condições forem atendidas:

- A Instância reservada não pode ser modificada antes ou ao mesmo tempo da compra
- a Instância reservada deve estar ativa.
- Não pode haver uma solicitação de modificação pendente
- A instância reservada não está listada no Marketplace de instâncias reservadas
- As Instâncias reservadas de entrada são todas Instâncias reservadas standard ou todas as Instâncias reservadas conversíveis, e não algumas de cada tipo
- As Instâncias reservadas de entrada deverão expirar na mesma hora, se forem Instâncias reservadas standard
- A Instância reservada não é uma instância do G4.

Enviar solicitações de modificação

Antes de modificar as instâncias reservadas, leia as [restrições \(p. 290\)](#) aplicáveis.

New console

Para modificar as instâncias reservadas usando o AWS Management Console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na página Reserved Instances (Instâncias reservadas), selecione uma ou mais Instâncias reservadas para modificar e escolha Actions (Ações), Modify Reserved Instances (Modificar instâncias reservadas).

Note

Se as Instâncias reservadas não estiverem no estado ativo ou não puderem ser modificadas, a opção Modificar Instâncias reservadas estará desativada.

3. A primeira entrada na tabela de modificação exibe os atributos da Instâncias reservadas selecionada e pelo menos uma configuração de destino abaixo dela. A coluna Unidades exibe o espaço para tamanho total da instância. Escolha Adicionar para cada nova configuração a ser adicionada. Modifique os atributos conforme necessário para cada configuração.
 - Scope (Escopo): escolha se a configuração se aplica a uma zona de disponibilidade ou a toda a região.
 - Zona de disponibilidade: Escolha a zona de disponibilidade necessária. Não aplicável para Instâncias reservadas regionais.
 - Count (Contagem): especifique o número de instâncias. Para dividir as Instâncias reservadas em várias configurações, reduza a contagem, escolha Add (Adicionar) e especifique uma contagem para a configuração adicional. Por exemplo, se você tiver uma única configuração com uma contagem de 10, poderá alterar sua contagem para 6 e adicionar uma configuração

com uma contagem de 4. Esse processo desativa a Instância reservada original assim que as novas Instâncias reservadas são ativadas.

4. Escolha Continue.
5. Para confirmar suas escolhas quando terminar de especificar as configurações de destino, selecione Submit modifications (Enviar modificações).
6. Você pode determinar o status de sua solicitação da modificação analisando a coluna State (Estado) na tela de Instâncias reservadas. Os estados possíveis são os seguintes.
 - ativo (modificação pendente) — estado de transição das Instâncias reservadas originais.
 - desativado (modificação pendente) — estado de transição das Instâncias reservadas originais enquanto as novas Instâncias reservadas são criadas
 - desativado — Instâncias reservadas modificadas e substituídas com êxito
 - ativo — uma das seguintes opções:
 - Novas Instâncias reservadas criadas com base em uma solicitação de modificação bem-sucedida
 - Instâncias reservadas originais após falha na solicitação da modificação

Old console

Para modificar as instâncias reservadas usando o AWS Management Console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na página Reserved Instances (Instâncias reservadas), selecione uma ou mais Instâncias reservadas para modificar e escolha Actions (Ações), Modify Reserved Instances (Modificar instâncias reservadas).

Note

Se as Instâncias reservadas não estiverem no estado ativo ou não puderem ser modificadas, a opção Modificar Instâncias reservadas estará desativada.

3. A primeira entrada na tabela de modificação exibe os atributos das Instâncias reservadas selecionadas e pelo menos uma configuração de destino abaixo dela. A coluna Unidades exibe o espaço para tamanho total da instância. Escolha Adicionar para cada nova configuração a ser adicionada. Modifique os atributos conforme o necessário para cada configuração e selecione Continue (Continuar):
 - Scope (Escopo): escolha se a configuração se aplica a uma zona de disponibilidade ou a toda a região.
 - Zona de disponibilidade: Escolha a zona de disponibilidade necessária. Não aplicável para Instâncias reservadas regionais.
 - Count (Contagem): especifique o número de instâncias. Para dividir as Instâncias reservadas em várias configurações, reduza a contagem, escolha Add (Adicionar) e especifique uma contagem para a configuração adicional. Por exemplo, se você tiver uma única configuração com uma contagem de 10, poderá alterar sua contagem para 6 e adicionar uma configuração com uma contagem de 4. Esse processo desativa a Instância reservada original assim que as novas Instâncias reservadas são ativadas.
4. Para confirmar suas escolhas quando terminar de especificar as configurações de destino, selecione Submit modifications (Enviar modificações).
5. Você pode determinar o status de sua solicitação da modificação analisando a coluna State (Estado) na tela de Instâncias reservadas. Os estados possíveis são os seguintes.
 - ativo (modificação pendente) — estado de transição das Instâncias reservadas originais.
 - desativado (modificação pendente) — estado de transição das Instâncias reservadas originais enquanto as novas Instâncias reservadas são criadas

- desativado — Instâncias reservadas modificadas e substituídas com êxito
- ativo — uma das seguintes opções:
 - Novas Instâncias reservadas criadas com base em uma solicitação de modificação bem-sucedida
 - Instâncias reservadas originais após falha na solicitação da modificação

Como modificar as Instâncias reservadas usando a linha de comando

1. Para modificar as Instâncias reservadas, você pode usar um dos comandos a seguir:
 - [modify-reserved-instances](#) (AWS CLI)
 - [Edit-EC2ReservedInstance](#) (AWS Tools for Windows PowerShell)
2. Para obter o status da modificação (`processing`, `fulfilled` ou `failed`) use um dos comandos a seguir:
 - [describe-reserved-instances-modifications](#) (AWS CLI)
 - [Get-EC2ReservedInstancesModification](#) (AWS Tools for Windows PowerShell)

Solucionar problemas de solicitações de modificação

Se as configurações de destino solicitadas forem exclusivas, você receberá uma mensagem de que sua solicitação está sendo processada. Neste ponto, o Amazon EC2 só determinou que os parâmetros da sua solicitação de modificação são válidos. A solicitação da modificação ainda pode falhar durante o processo em função de capacidade indisponível.

Em algumas situações, você pode receber uma mensagem indicando solicitações de modificação incompletas ou falhas em vez de confirmação. Use as informações nessas mensagens como ponto inicial para enviar novamente outra solicitação de modificação. Certifique-se de que você leu as [restrições \(p. 290\)](#) aplicáveis antes de enviar a solicitação.

Nem todas as Instâncias reservadas selecionadas podem ser processadas para modificação

O Amazon EC2 identifica e lista as Instâncias reservadas que não podem ser modificadas. Se você receber uma mensagem como essa, acesse a página Reserved Instances (Instâncias reservadas) no console do Amazon EC2 e verifique as informações sobre as Instâncias reservadas.

Erro ao processar sua solicitação de modificação

Você enviou uma ou mais Instâncias reservadas para modificação e nenhuma das solicitações pode ser processada. Dependendo do número de reservas que estiver modificando, você pode obter versões diferentes da mensagem.

O Amazon EC2 exibe os motivos pelos quais sua requisição não pode ser processada. Por exemplo, você pode ter especificado a mesma combinação de destino — uma combinação de zona de disponibilidade e plataforma — para um ou mais subconjuntos das Instâncias reservadas que está modificando. Experimente enviar as solicitações de modificação novamente, mas verifique se os detalhes da instância das reservas correspondem, e as configurações de destino para todos os subconjuntos que estiverem sendo modificados são exclusivas.

Trocar Instâncias reservadas conversíveis

Você pode trocar uma ou mais Instâncias reservadas conversíveis por outra Instância reservada convertível com uma configuração diferente, inclusive a família de instâncias, o sistema operacional e a locação. Não há limites de vezes para executar uma troca, desde que a nova Instância reservada convertível tenha valor igual ou superior às Instâncias reservadas conversíveis que você está trocando.

Ao trocar sua instância reservada conversível, o número de instâncias da sua reserva atual é trocado por um número de instâncias que cobrem o valor igual ou superior da configuração da nova instância reservada conversível. O Amazon EC2 calcula o número de instâncias reservadas que você pode receber como resultado da troca.

Você não pode trocar Instâncias reservadas padrão, mas pode modificá-las. Para obter mais informações, consulte [Modificar a Instâncias reservadas \(p. 289\)](#).

Tópicos

- [Requisitos para trocar de Instâncias reservadas conversíveis \(p. 294\)](#)
- [Calcular trocas de Instâncias reservadas conversíveis \(p. 295\)](#)
- [Mesclar Instâncias reservadas conversíveis \(p. 296\)](#)
- [Trocá uma parte de uma Instância reservada convertível \(p. 296\)](#)
- [Enviar solicitações de troca \(p. 297\)](#)

[Requisitos para trocar de Instâncias reservadas conversíveis](#)

Se as condições a seguir forem atendidas, o Amazon EC2 processará sua solicitação de troca. A Instância reservada convertível deve estar:

- Ativo
- Não pode haver uma solicitação de troca anterior pendente

As seguintes regras se aplicam:

- As instâncias reservadas conversíveis só podem ser trocadas por outras instâncias reservadas conversíveis oferecidas atualmente pela AWS.
- As Instâncias reservadas conversíveis são associadas a uma região específica, que é fixada para a duração do período da reserva. Não é possível trocar uma Instância reservada convertível por uma Instância reservada convertível de outra região.
- Você pode trocar uma ou mais Instâncias reservadas conversíveis por vez por uma única Instância reservada convertível somente.
- Para trocar parte de uma Instância reservada convertível, você pode modificá-la em duas ou mais reservas e, em seguida, trocar uma ou mais reservas por uma nova Instância reservada convertível. Para obter mais informações, consulte [Trocá uma parte de uma Instância reservada convertível \(p. 296\)](#). Para obter mais informações sobre como modificar Instâncias reservadas, consulte [Modificar a Instâncias reservadas \(p. 289\)](#).
- As Instâncias reservadas conversíveis com adiantamento total podem ser trocadas por Instâncias reservadas conversíveis com adiantamentos parciais e vice-versa.

Note

Se o pagamento adiantado total necessário para a troca (custo alinhado) for menor do que 0,00 USD, a AWS fornecerá automaticamente uma quantidade de instâncias na instância reservada conversível que garantirá o custo alinhado de 0,00 USD ou mais.

Note

Se o valor total (preço adiantado + preço por hora * número de horas restantes) da nova instância reservada conversível for menor do que o valor total da instância reservada conversível que foi trocada, a AWS fornecerá automaticamente uma quantidade de instâncias na instância reservada conversível que garantirá um valor total igual ou superior ao valor da instância reservada conversível trocada.

- Para se beneficiar com preços melhores, você pode trocar uma Instância reservada convertível sem adiantamento por uma Instância reservada convertível com adiantamento total ou parcial.

- Você não pode trocar Instâncias reservadas conversíveis com adiantamento total e parcial por Instâncias reservadas conversíveis sem adiantamento.
- Só é possível trocar uma Instância reservada convertível sem adiantamento por uma outra Instância reservada convertível sem adiantamento se o preço por hora da nova Instância reservada convertível for igual ou superior ao preço por hora da Instância reservada convertível que foi trocada.

Note

Se o valor total (preço por hora * número de horas restantes) da nova instância reservada conversível for menor do que o valor total da instância reservada conversível que foi trocada, a AWS fornecerá automaticamente uma quantidade de instâncias na instância reservada conversível que garantirá um valor total igual ou superior ao valor da instância reservada conversível trocada.

- Se você trocar várias Instâncias reservadas conversíveis com datas de expiração diferentes, a data de expiração da nova Instância reservada convertível será a data futura mais longe.
- Se você trocar uma única Instância reservada convertível, ela deverá ter o mesmo período de vigência (um ano ou três anos) da nova Instância reservada convertível. Se você mesclar várias Instâncias reservadas conversíveis com períodos de vigência diferentes, a nova Instância reservada convertível terá um período de vigência de três anos. Para obter mais informações, consulte [Mesclar Instâncias reservadas conversíveis \(p. 296\)](#).
- Depois de trocar um Instância reservada convertível, a reserva original é desativada. A data final é a data inicial da nova reserva, e a data final da nova reserva é a mesma que a data final da Instância reservada convertível original. Por exemplo, se você modificar uma reserva de três anos com 16 meses restando do período de vigência, a reserva modificada resultante será uma reserva de 16 meses com a mesma data final que a original.

Calcular trocas de Instâncias reservadas conversíveis

A troca de Instâncias reservadas conversíveis são gratuitas. No entanto, pode ser obrigado a pagar um custo alinhado, que é o custo adiantado pro rata da diferença entre as Instâncias reservadas conversíveis que você tinha e as novas Instâncias reservadas conversíveis que você recebe da troca.

Cada Instância reservada convertível tem um valor de tabela. Esse valor de tabela é comparado ao valor de tabela das Instâncias reservadas conversíveis que você deseja para determinar quantas reservas de instância você pode receber com a troca.

Por exemplo: você tem uma Instância reservada convertível com valor de tabela de 35 USD que deseja trocar por um novo tipo de instância com um valor de tabela de 10 USD.

\$35/\$10 = 3.5

Você pode trocar sua Instância reservada convertível por três Instâncias reservadas conversíveis de US \$ 10. Não é possível adquirir meias reservas; portanto, é necessário comprar uma Instância reservada convertível adicional que cubra o restante:

3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved Instance

A quarta Instância reservada convertível tem a mesma data de término das outras três. Se você estiver trocando Instâncias reservadas conversíveis com adiantamento integral ou parcial, pagará o custo alinhado da quarta reserva. Se os custos iniciais restante das Instâncias reservadas conversíveis forem \$ 500 e a reserva de destino custar normalmente \$ USD pro rata, será cobrado de você \$ 100.

\$600 prorated upfront cost of new reservations - \$500 remaining upfront cost of original reservations = \$100 difference

Mesclar Instâncias reservadas conversíveis

Se você mesclar duas ou mais Instâncias reservadas conversíveis, o termo da nova Instância reservada convertível deverá ser o mesmo que a Instâncias reservadas conversíveis original, ou o mais alto da Instâncias reservadas conversíveis original. A data de expiração da nova Instância reservada convertível é a data de expiração mais avançada no futuro.

Por exemplo, você tem as seguintes Instâncias reservadas conversíveis na conta:

ID da Instância reservada	Prazo	Data de validade
aaaa1111	1 ano	31/12/2018
bbbb2222	1 ano	31/07/2018
cccc3333	3 anos	30/06/2018
dddd4444	3 anos	31/12/2019

- Você pode mesclar aaaa1111 e bbbb2222 e trocá-las por uma Instância reservada convertível de um ano. Você não pode trocá-las por uma Instância reservada convertível de três anos. A data de expiração da nova Instância reservada convertível é 31/12/2018.
- Você pode mesclar bbbb2222 e cccc3333 e trocá-las por uma Instância reservada convertível de três anos. Você não pode trocá-las por uma Instância reservada convertível de um ano. A data de expiração da nova Instância reservada convertível é 31/07/2018.
- Você pode mesclar cccc3333 e dddd4444 e trocá-las por uma Instância reservada convertível de três anos. Você não pode trocá-las por uma Instância reservada convertível de um ano. A data de expiração da nova Instância reservada convertível é 31/12/2019.

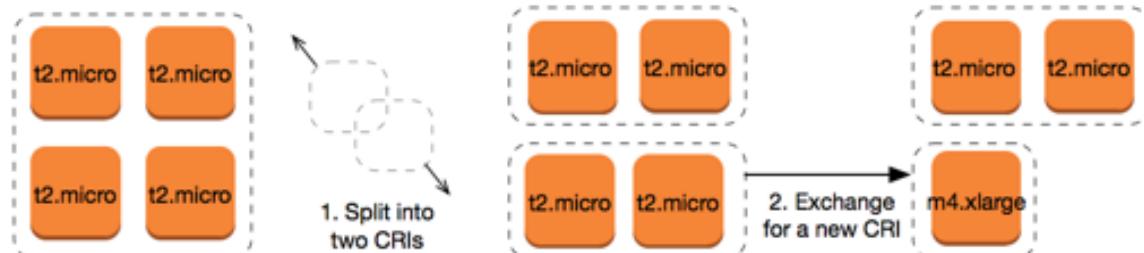
Trocar uma parte de uma Instância reservada convertível

Você pode usar o processo de modificação para dividir a Instância reservada convertível em reservas menores e, em seguida, trocar uma ou mais reservas novas por uma nova Instância reservada convertível. Os exemplos a seguir demonstram como fazer isso.

Example Exemplo: Instância reservada convertível com várias instâncias

Neste exemplo, você tem uma t2.micro Instância reservada convertível com quatro instâncias na reserva. Para trocar duas instâncias t2.micro por uma instância m4.xlarge:

1. Modifique a t2.micro Instância reservada convertível dividindo-a em duas t2.micro Instâncias reservadas conversíveis com duas instâncias cada uma.
2. Troque uma das novas t2.micro Instâncias reservadas conversíveis por uma m4.xlarge Instância reservada convertível.



Enviar solicitações de troca

Você pode trocar as Instâncias reservadas conversíveis usando o console do Amazon EC2 ou uma ferramenta de linha de comando.

Troque uma Instância reservada convertível usando o console

Você pode procurar ofertas de Instâncias reservadas conversíveis e selecionar sua nova configuração entre as escolhas apresentadas.

New console

Para trocar Instâncias reservadas conversíveis usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Instâncias reservadas, selecione as Instâncias reservadas conversíveis a serem trocadas e escolha Ações, Trocar Instância reservada.
3. Selecione os atributos da configuração desejada e escolha Find offering (Localizar oferta).
4. Selecione uma nova Instância reservada convertível. Na parte inferior da tela, você pode visualizar o número da Instâncias reservadas que você receber para a troca, além de quaisquer custos adicionais.
5. Ao selecionar uma Instância reservada convertível que atenda às suas necessidades, escolha Review (Revisar).
6. Escolha Exchange (Troca) e, em seguida, Close (Fechar).

Old console

Para trocar Instâncias reservadas conversíveis usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Instâncias reservadas, selecione as Instâncias reservadas conversíveis a serem trocadas e escolha Ações, Trocar Instância reservada.
3. Selecione os atributos da configuração desejada e escolha Find Offering (Localizar oferta).
4. Selecione uma nova Instância reservada convertível. A coluna Instance Count (Contagem de instâncias) exibirá o número de Instâncias reservadas que você recebe pela troca. Ao selecionar uma Instância reservada convertível que atenda às suas necessidades, escolha Exchange (Troca).

As Instâncias reservadas que foram trocadas foram eliminadas e as novas Instâncias reservadas são exibidas no console do Amazon EC2. Esse processo pode levar alguns minutos para ser propagado.

Trocando uma Instância reservada convertível usando a interface da linha de comando

Para trocar uma Instância reservada convertível, primeiro localize uma Instância reservada convertível de destino que atenda às suas necessidades:

- [describe-reserved-instances-offerings](#) (AWS CLI)
- [Get-EC2ReservedInstancesOffering](#) (Tools for Windows PowerShell)

Obtenha uma cotação para a troca, que inclua o número de Instâncias reservadas obtidas na troca e o custo alinhado da troca:

- [get-reserved-instances-exchange-quote](#) (AWS CLI)
- [GetEC2-ReservedInstancesExchangeQuote](#) (Tools for Windows PowerShell)

Por fim, execute a troca:

- [accept-reserved-instances-exchange-quote](#) (AWS CLI)
- [Confirm-EC2ReservedInstancesExchangeQuote](#) (Tools for Windows PowerShell)

Scheduled Reserved Instances

Com instâncias reservadas programadas, é possível reservar capacidade programada para se repetir diariamente, semanalmente ou mensalmente, com uma hora de início e duração especificadas, pelo prazo de um ano. Depois de concluir a compra, as instâncias estarão disponíveis para serem iniciadas durante as janelas de tempo especificadas.

Important

Não é possível comprar instâncias reservadas programadas no momento. A AWS não tem capacidade disponível para instâncias reservadas programadas ou planos para disponibilizá-las no futuro. Para reservar capacidade, use [On-Demand Capacity Reservations \(p. 390\)](#), em vez disso. Para taxas com desconto, use o [Savings Plans](#).

Spot Instances

Uma instância spot é uma instância que usa capacidade adicional do EC2 que está disponível por um valor mais baixo que o preço sob demanda. Como as Instâncias spot permitem que você solicite instâncias do EC2 não usadas com descontos consideráveis, você pode reduzir seus custos do Amazon EC2 significativamente. O preço por hora de uma instância spot é chamado de preço spot. O preço spot de cada tipo de instância em cada zona de disponibilidade é definido pelo Amazon EC2 e ajustado gradualmente com base na oferta e a demanda de longo prazo das Instâncias spot. Sua instância spot é executada sempre que a capacidade está disponível e o preço máximo por hora da sua solicitação excede o preço spot.

As Instâncias spot são uma opção econômica se houver flexibilidade quanto ao momento em que as aplicações serão executadas e se as aplicações poderão ser interrompidas. Por exemplo, as Instâncias spot são adequadas para análise de dados, trabalhos em lote, processamento em segundo plano e tarefas opcionais. Para obter mais informações, consulte [Instâncias spot do Amazon EC2](#).

Tópicos

- [Concepts \(p. 299\)](#)
- [Como começar a usar \(p. 300\)](#)
- [Serviços relacionados \(p. 301\)](#)
- [Definição de preço e economia \(p. 301\)](#)

Concepts

Antes de começar a trabalhar com as Instâncias spot, você deve se familiarizar com os seguintes conceitos:

- Grupo de capacidade spot: um conjunto de instâncias do EC2 não utilizadas com o mesmo tipo de instância (por exemplo, `m5.large`) e zona de disponibilidade.
- Preço spot: o preço atual de uma instância spot por hora.
- Solicitação de instância Spot: solicita uma instância spot. A solicitação fornece o preço máximo por hora que você está disposto a pagar por uma instância spot. Se você não especificar um preço máximo, o padrão será o preço sob demanda. Quando o preço máximo por hora da sua solicitação excede o preço spot, o Amazon EC2 atende à sua solicitação mediante a disponibilidade de capacidade. Uma solicitação de instância spot é única ou persistente. O Amazon EC2 reenvia automaticamente uma solicitação de instância spot persistente depois que a instância spot associada à solicitação é encerrada.
- Recomendação de rebalanceamento de instância do EC2: o Amazon EC2 emite um sinal de recomendação de rebalanceamento de instância para avisar que uma instância spot possui risco elevado de interrupção. Esse sinal fornece a oportunidade de rebalancear proativamente os workloads entre instâncias spot novas ou existentes sem ter que aguardar o aviso de interrupção de dois minutos da instância spot.
- Interrupção de instância spot: o Amazon EC2 encerra, interrompe ou coloca em hibernação a instância spot quando o Amazon EC2 precisa da capacidade ou o preço spot excede o preço máximo de sua solicitação. O Amazon EC2 fornece um aviso de interrupção da instância spot, enviando à instância um aviso de dois minutos antes que ela seja interrompida.

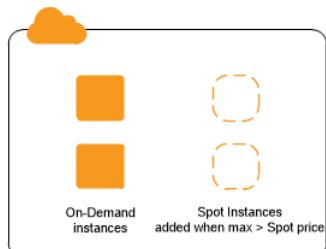
Principais diferenças entre Instâncias spot e Instâncias on-demand

A tabela a seguir lista as principais diferenças entre Instâncias spot e Instâncias on-demand.

	Spot Instances	On-Demand Instances
Horário do lançamento	Só poderá ser executado imediatamente se a solicitação da instância spot estiver ativa e a capacidade estiver disponível.	Só poderá ser executado imediatamente se você fizer uma solicitação de execução manual e se a capacidade estiver disponível.
Capacidade disponível	Se a capacidade não estiver disponível, a solicitação de instância spot continuará a fazer a solicitação de inicialização automaticamente até que a capacidade seja disponibilizada.	Se a capacidade não estiver disponível quando você fizer uma solicitação de execução, você receberá um erro de capacidade insuficiente (ICE).
Custo por hora	O preço por hora de Instâncias spot varia de acordo com a demanda.	O preço por hora de Instâncias on-demand é estático.
Recomendação de rebalanceamento	O sinal que o Amazon EC2 emite para uma instância spot em execução quando a instância possui risco elevado de interrupção.	Você determina quando uma instância sob demanda é interrompida (parada ou encerrada).
Interrupção de instância	É possível interromper e iniciar uma instância spot com Amazon EBS. Além disso, o serviço spot do Amazon EC2 poderá interromper (p. 336) uma instância spot individual se a capacidade não estiver mais disponível, o preço spot exceder seu preço máximo ou a demanda por instâncias spot aumentar.	Você determina quando uma instância sob demanda é interrompida (parada ou encerrada).

Estratégias para usar Instâncias spot

Uma estratégia para manter um nível mínimo de recursos de computação garantidos para as aplicações é executar um grupo principal de Instâncias on-demand e complementá-los com Instâncias spot quando surgir a oportunidade.



Comparar instâncias sob demanda e Instâncias spot

Como começar a usar

A primeira coisa que você precisa fazer é configurar o Amazon EC2 para ser usado. Também pode ser útil testar a execução de Instâncias on-demand antes de executar Instâncias spot.

Comece já

- [Configuração para usar o Amazon EC2. \(p. 6\)](#)
- [Tutorial: Comece a usar instâncias Windows do Amazon EC2 \(p. 10\)](#)

Noções básicas do spot

- [Como as Instâncias spot funcionam \(p. 304\)](#)

Trabalho com Instâncias spot

- [Preparar-se para interrupções \(p. 340\)](#)
- [Criar uma solicitação de instância spot \(p. 313\)](#)
- [Obter informações do status da solicitação \(p. 331\)](#)

Serviços relacionados

Você pode provisionar Instâncias spot usando diretamente o Amazon EC2. Você pode provisionar as instâncias spot usando outros serviços da AWS. Para obter mais informações, consulte a documentação a seguir.

Amazon EC2 Auto Scaling e Instâncias spot

É possível criar configurações ou modelos de execução com o preço máximo que está disposto a pagar para que o Amazon EC2 Auto Scaling possa executar as Instâncias spot. Para obter mais informações, consulte [Solicitar Instâncias spot aplicações flexíveis e tolerantes a falhas e Auto Scaling grupos com vários tipos de instância e opções de compra](#) no Guia do usuário do Amazon EC2 Auto Scaling.

Amazon EMR e Instâncias spot

Há cenários em que pode ser útil executar Instâncias spot em um cluster do Amazon EMR. Para obter mais informações, consulte [Instâncias spot](#) e [Quando você deve usar Instâncias spot](#) no Guia de gerenciamento do Amazon EMR.

AWS CloudFormation Modelos do

O AWS CloudFormation permite criar e gerenciar uma coleção de recursos da AWS usando um modelo em formato JSON. Os modelos do AWS CloudFormation podem incluir o preço máximo que você quer pagar. Para obter mais informações, consulte [EC2 Spot Instance Updates - Auto Scaling and CloudFormation Integration \(Atualizações de instâncias spot do EC2: integração do Auto Scaling e do CloudFormation\)](#).

AWS SDK for Java

Você pode usar a linguagem de programação Java para gerenciar as Instâncias spot. Para obter mais informações, consulte [Tutorial: Instâncias spot do Amazon EC2](#) e [Tutorial: Gerenciamento avançado de solicitações spot do Amazon EC2](#).

AWS SDK for .NET

Você pode usar o ambiente de programação .NET para gerenciar as Instâncias spot. Para obter mais informações, consulte [Tutorial: Instâncias spot do Amazon EC2](#).

Definição de preço e economia

Você paga o preço spot por Instâncias spot, que é definido pelo Amazon EC2 e ajustado gradualmente com base na oferta e demanda de longo prazo das Instâncias spot. Se o preço máximo da sua solicitação exceder o preço spot atual, o Amazon EC2 atenderá à sua solicitação mediante a disponibilidade de capacidade. Suas Instâncias spot serão executadas até que você as encerre, a capacidade não esteja mais disponível, o preço spot exceda o seu preço máximo ou seu grupo do Amazon EC2 Auto Scaling as encerre durante o [ajuste de escala](#).

Se você ou o Amazon EC2 interromper uma instância spot em execução, você será cobrado pelos segundos usados ou pela hora completa, ou então não será cobrado, dependendo do sistema operacional usado e de quem interrompeu a instância spot. Para obter mais informações, consulte [Faturamento para Instâncias spot interrompidas \(p. 344\)](#).

Visualizar preços

Para visualizar o menor preço spot atual (atualizado a cada cinco minutos) por região da AWS e tipo de instância, consulte a página [Definição de preço de instâncias spot do Amazon EC2](#).

Para visualizar o histórico de preços spot dos últimos três meses, use o console do Amazon EC2 ou o comando `describe-spot-price-history` (AWS CLI). Para obter mais informações, consulte [Histórico de definição de preço da instância spot \(p. 306\)](#).

Mapeamos as zonas de disponibilidade para os códigos de cada conta da AWS de forma independente. Portanto, você pode obter resultados diferentes para o mesmo código de zona de disponibilidade (por exemplo, `us-west-2a`) entre contas diferentes.

Visualizar economias

Você pode visualizar as economias feitas com o uso de instâncias spot para uma única frota spot ou para todas as instâncias spot. Você pode visualizar as economias feitas na última hora ou nos últimos três dias, além de visualizar o custo médio por hora de vCPU e por hora de memória (GiB). As economias são estimadas e podem ser diferentes das economias reais porque não incluem os ajustes de faturamento de seu uso. Para obter mais informações sobre a visualização das economias, consulte [Economia na compra das Instâncias spot \(p. 307\)](#).

Exibir faturamento

Sua fatura fornece detalhes sobre seu uso do serviço. Para obter mais informações, consulte [Viewing your bill](#) (Visualizar sua fatura) no AWS Billing and Cost Management User Guide (Manual do usuário do AWS Billing and Cost Management).

Melhores práticas para o EC2 Spot

Os instâncias spot do Amazon EC2 representam a capacidade computacional adicional do EC2 na Nuvem AWS que está disponível para você com um desconto de até 90% em comparação aos preços sob demanda. A única diferença entre Instâncias on-demand e Instâncias spot é que as Instâncias spot podem ser interrompidas pelo Amazon EC2, com dois minutos de notificação, quando o Amazon EC2 precisa da capacidade de volta.

As Instâncias spot são recomendadas para aplicações flexíveis, tolerantes a falhas e sem estado. Por exemplo, as Instâncias spot funcionam bem para big data, workloads em contêineres, CI/CD, servidores Web sem estado, computação de alta performance (HPC) e workloads de renderização.

Durante a execução, as Instâncias spot são exatamente as mesmos que as Instâncias on-demand. No entanto, o Spot não garante que você possa manter as instâncias em execução tempo suficiente para concluir as workloads. O Spot também não garante que você possa obter disponibilidade imediata das instâncias que está procurando, nem que sempre possa obter a capacidade agregada solicitada. Além disso, as interrupções e a capacidade da instância spot podem mudar ao longo do tempo porque a disponibilidade da instância spot varia de acordo com a oferta e a demanda, e a performance passada não é uma garantia de resultados futuros.

As Instâncias spot não são adequadas para workloads que são inflexíveis, com estado, intolerantes a falhas ou fortemente acopladas entre nós de instância. Elas também não são recomendadas para workloads intolerantes a períodos ocasionais quando a capacidade de destino não está completamente disponível. Não recomendamos o uso de Instâncias spot para essas workloads nem a tentativa de executar failover para Instâncias on-demand a fim de lidar com interrupções.

Independentemente de você ser um usuário spot experiente ou iniciante na utilização de instâncias spot, se estiver enfrentando problemas com interrupções ou disponibilidade de instâncias spot no momento, recomendamos que siga essas práticas recomendadas para ter a melhor experiência usando o serviço spot.

Melhores práticas do Spot

- [Preparar instâncias individuais para interrupções \(p. 303\)](#)
- [Ser flexível sobre tipos de instância e zonas de disponibilidade \(p. 303\)](#)
- [Usar grupos do EC2 Auto Scaling ou frota spot para gerenciar a capacidade agregada \(p. 304\)](#)
- [Usar a estratégia de alocação otimizada por capacidade \(p. 304\)](#)
- [Usar rebalanceamento proativo de capacidade \(p. 304\)](#)
- [Usar produtos integrados da AWS para gerenciar as instâncias spot \(p. 304\)](#)

Preparar instâncias individuais para interrupções

A melhor maneira de lidar com interrupções de instâncias spot com tranquilidade é arquitetar a aplicação para que ela seja tolerante a falhas. Para fazer isso, você pode aproveitar as recomendações de rebalanceamento de instâncias do EC2 e avisos de interrupção de instâncias spot.

Uma recomendação de rebalanceamento de uma instância do EC2 é um novo sinal que avisa quando uma instância spot tem risco elevado de interrupção. O sinal oferece a oportunidade de gerenciar proativamente a instância spot antes do aviso de interrupção de dois minutos da instância spot. Você pode decidir rebalancear sua workload em Instâncias spot novas ou existentes que não tenham risco elevado de interrupção. O uso desse sinal ficou mais fácil com o uso do recurso de Rebalanceamento de capacidade em grupos de Auto Scaling e frota spot. Para obter mais informações, consulte [Usar rebalanceamento proativo de capacidade \(p. 304\)](#).

Um aviso de interrupção da instância spot é um aviso emitido dois minutos antes de o Amazon EC2 interromper uma instância spot. Se a workload tiver “flexibilidade de tempo”, você também poderá configurar as instâncias Spot para serem interrompidas ou para hibernarem, em vez de serem encerradas, quando forem interrompidas. O Amazon EC2 interrompe ou hiberna automaticamente suas instâncias spot durante a interrupção e retoma automaticamente as instâncias quando tivermos capacidade disponível.

Recomendamos que você crie uma regra no [Amazon EventBridge](#) que capture as recomendações de rebalanceamento e os avisos de interrupção e acione um ponto de verificação para o andamento da workload ou lide tranquilamente com a interrupção. Para obter mais informações, consulte [Monitorar os sinais de recomendação de rebalanceamento \(p. 334\)](#). Para obter um exemplo detalhado que orienta você sobre como criar e usar regras de evento, consulte [Aproveitar os avisos de interrupção de instância spot do Amazon EC2](#).

Para obter mais informações, consulte [Recomendações de rebalanceamento de instâncias do EC2 \(p. 333\)](#) e [Interrupções de instâncias spot \(p. 336\)](#).

Ser flexível sobre tipos de instância e zonas de disponibilidade

Um grupo de capacidade spot é um conjunto de instâncias do EC2 não utilizadas com o mesmo tipo de instância (por exemplo, m5.large) e zona de disponibilidade (por exemplo, us-east-1a). Você deve ser flexível sobre quais tipos de instância solicita e em quais zonas de disponibilidade pode implantar a workload. Isso dá ao Spot uma chance melhor de encontrar e alocar a quantidade necessária de capacidade computacional. Por exemplo, não peça apenas c5.large se você está disposto a usar grandes das famílias c4, m5 e m4.

Dependendo de suas necessidades específicas, é possível avaliar para quais tipos de instância você pode ter flexibilidade para atender aos requisitos de computação. Se uma workload puder ser dimensionada verticalmente, você deve incluir tipos de instância maiores (mais vCPUs e memória) nas solicitações. Se você puder dimensionar somente horizontalmente, deverá incluir tipos de instância de geração mais antiga, pois eles têm menos demanda de clientes sob demanda.

Uma boa regra geral é ser flexível para pelo menos 10 tipos de instância para cada workload. Além disso, verifique se todas as zonas de disponibilidade estão configuradas para uso na VPC e selecionadas para a workload.

Usar grupos do EC2 Auto Scaling ou frota spot para gerenciar a capacidade agregada

O spot permite que você pense em termos de capacidade agregada, ou seja, em unidades que incluem vCPUs, memória, armazenamento ou taxa de transferência de rede, em vez de pensar em termos de instâncias individuais. Os grupos do Auto Scaling e a frota spot permitem que você execute e mantenha uma capacidade pretendida e solicite automaticamente recursos para substituir qualquer uma que seja interrompida ou encerrada manualmente. Ao configurar um grupo do Auto Scaling ou uma frota spot, você só precisa especificar os tipos de instância e a capacidade pretendida com base nas necessidades da aplicação. Para obter mais informações, consulte [Grupos de Auto Scaling](#) no Guia do usuário do Amazon EC2 Auto Scaling e [Criar uma solicitação de frota spot \(p. 776\)](#) neste guia do usuário.

Usar a estratégia de alocação otimizada por capacidade

As estratégias de alocação nos grupos de Auto Scaling ajudam a provisionar a capacidade prevista sem a necessidade de procurar manualmente os grupos de capacidade spot com capacidade adicional. Recomendamos o uso da estratégia `capacity optimized`, pois ela provisão automaticamente as instâncias dos grupos de capacidade spot mais disponíveis. Também é possível aproveitar a estratégia de alocação `capacity optimized` na frota spot. Como a capacidade da instância spot é proveniente de grupos com capacidade ideal, isso diminui a possibilidade de que as instâncias spot sejam recuperadas. Para obter mais informações sobre estratégias de alocação, consulte [Instâncias spot](#) no Guia do usuário do Amazon EC2 Auto Scaling e [Configurar a frota spot para otimização de capacidade \(p. 764\)](#) neste guia do usuário.

Usar rebalanceamento proativo de capacidade

O Rebalanceamento de capacidade ajuda a manter a disponibilidade da workload aumentando proativamente sua frota com uma nova instância spot antes que uma instância spot em execução receba o aviso de interrupção de dois minutos. Quando o Rebalanceamento de capacidade está habilitado, o Auto Scaling ou a Frota spot tenta substituir proativamente as Instâncias spot que receberam uma recomendação de rebalanceamento, oferecendo a oportunidade de rebalancear a workload para novas Instâncias spot que não apresentam risco elevado de interrupção.

O Rebalanceamento de capacidade complementa a estratégia de alocação otimizada de capacidade (criada para ajudar a encontrar a capacidade de reserva ideal) e a política de instâncias mistas (criada para aumentar a disponibilidade ao implantar instâncias em vários tipos de instância executados em várias zonas de disponibilidade).

Para obter mais informações, consulte [Rebalanceamento de capacidade \(p. 765\)](#).

Usar produtos integrados da AWS para gerenciar as instâncias spot

Outros serviços da AWS integram-se ao Spot para reduzir os custos gerais de computação sem a necessidade de gerenciar instâncias ou frotas individuais. Recomendamos que você considere as seguintes soluções para as workloads aplicáveis: Amazon EMR, Amazon ECS, AWS Batch, Amazon EKS, SageMaker, AWS Elastic Beanstalk e Amazon GameLift. Para saber mais sobre as melhores práticas do Spot com esses serviços, consulte o [Site de workshops de Instâncias spot do Amazon EC2](#).

Como as Instâncias spot funcionam

Para iniciar uma instância Spot, você cria uma solicitação de instância spot ou o Amazon EC2 cria uma solicitação de instância spot em seu nome. A instância spot é iniciada quando a solicitação de instância spot é atendida.

Você pode iniciar uma instância spot usando vários serviços diferentes. Para obter mais informações, consulte [Conceitos básicos das instâncias spot do Amazon EC2](#). Neste guia do usuário, descrevemos as seguintes maneiras de executar uma instância spot usando o EC2:

- Você pode criar uma solicitação de instância spot. Para obter mais informações, consulte [Criar uma solicitação de instância spot \(p. 313\)](#).
- Você pode criar uma EC2 Fleet e nela especificar o número desejado de instâncias spot. O Amazon EC2 cria uma solicitação de instância spot em seu nome para cada instância spot especificada na EC2 Fleet. Para obter mais informações, consulte [Criar uma Frota do EC2 \(p. 751\)](#).
- Você pode criar uma frota spot e nela especificar o número desejado de instâncias spot. O Amazon EC2 cria uma solicitação de instância spot em seu nome para cada instância spot especificada na solicitação de frota spot. Para obter mais informações, consulte [Criar uma solicitação de frota spot \(p. 776\)](#).

A solicitação de instância spot deve incluir o preço máximo que você está disposto a pagar por hora por instância. Caso você não especifique, o preço padrão será sob demanda. A solicitação pode incluir outras restrições, como o tipo de instância e a Zona de disponibilidade.

Sua instância spot será executada se o preço máximo que você estiver disposto a pagar exceder o preço spot e se houver capacidade disponível. Se o preço máximo que você estiver disposto a pagar for inferior ao preço spot, sua instância não será executada. No entanto, como o Amazon EC2 ajusta gradualmente o preço spot com base na oferta e demanda de longo prazo para Instâncias spot, o preço máximo que você está disposto a pagar poderá eventualmente exceder o preço spot, caso em que sua instância será executada.

Sua instância spot será executada até que você a interrompa ou a encerre, ou até que o Amazon EC2 a interrompa (processo conhecido como interrupção da instância spot).

Quando você usa instâncias spot, deve estar preparado para interrupções. O Amazon EC2 pode interromper a sua instância spot quando a demanda por instâncias spot aumentar, quando o fornecimento de instâncias spot diminuir ou quando o preço spot exceder o preço máximo. Quando o Amazon EC2 interrompe uma instância spot, ele fornece um aviso de interrupção de instância spot, enviando à instância um aviso de dois minutos antes que o Amazon EC2 a interrompa. Você não pode habilitar a proteção contra encerramento para Instâncias spot. Para obter mais informações, consulte [Interrupções de instâncias spot \(p. 336\)](#).

Você pode parar, iniciar, reiniciar ou encerrar uma instância com Amazon EBS. O serviço spot pode parar, encerrar ou hibernar uma instância spot quando a interrompe.

Tópicos

- [Executar Instâncias spot em um grupo de execução \(p. 305\)](#)
- [Executar Instâncias spot em um grupo de zonas de disponibilidade \(p. 306\)](#)
- [Executar Instâncias spot em uma VPC \(p. 306\)](#)

Executar Instâncias spot em um grupo de execução

Especifique um grupo de execução na solicitação de instância spot para instruir o Amazon EC2 a executar um conjunto de instâncias spot somente se ele puder executar todas elas. Além disso, se o serviço spot precisar encerrar uma das instâncias em um grupo de execução (por exemplo, se o preço spot exceder seu preço máximo), ele deverá encerrar todas elas. Contudo, se você encerrar uma ou mais instâncias em um grupo de execução, o Amazon EC2 não encerrará as instâncias restantes no grupo de execução.

Embora essa opção possa ser útil, adicionar essa restrição pode diminuir as chances de a sua solicitação de instância spot ser atendida e aumenta as chances de encerramento das instâncias spot. Por exemplo, seu grupo de execução inclui instâncias em várias zonas de disponibilidade. Se a capacidade em uma dessas zonas de disponibilidade diminuir e não estiver mais disponível, o Amazon EC2 encerrará todas as instâncias do grupo de execução.

Se você criar outra solicitação de instância spot bem-sucedida que especifique o mesmo grupo de execução (existente) de uma solicitação bem-sucedida anterior, as novas instâncias serão adicionadas ao grupo de execução. Subsequentemente, se uma instância nesse grupo de execução for encerrada, todas as instâncias no grupo de execução serão encerradas, o que inclui instâncias executadas pela primeira e a segunda solicitações.

Executar Instâncias spot em um grupo de zonas de disponibilidade

Especifique um grupo de zonas de disponibilidade na solicitação de instância spot para informar ao serviço spot para executar um conjunto de instâncias spot na mesma zona de disponibilidade. O Amazon EC2 não precisa interromper todas as instâncias em um grupo de zonas de disponibilidade ao mesmo tempo. Se o Amazon EC2 precisar interromper uma das instâncias em um grupo de zonas de disponibilidade, as outras permanecerão em execução.

Embora essa opção possa ser útil, a adição dessa restrição pode reduzir as possibilidades de sua solicitação de instância spot ser atendida.

Se você especificar um grupo de zonas de disponibilidade, mas não especificar uma zona de disponibilidade na solicitação de instância spot, o resultado dependerá da rede especificada.

VPC padrão

O Amazon EC2 usa a zona de disponibilidade para a sub-rede especificada. Se você não especificar uma sub-rede, ele selecionará uma zona de disponibilidade e sua sub-rede padrão, mas não necessariamente a zona de preço mais baixo. Se você excluir a sub-rede padrão de uma zona de disponibilidade, deverá especificar uma sub-rede diferente.

VPC não padrão

O Amazon EC2 usa a zona de disponibilidade para a sub-rede especificada.

Executar Instâncias spot em uma VPC

Especifique uma sub-rede para as Instâncias spot da mesma maneira que você especifica uma sub-rede para as Instâncias on-demand.

- Você deve usar o preço máximo padrão (preço sob demanda) ou basear seu preço máximo no histórico de preços spot das Instâncias spot em uma VPC.
- [VPC padrão] Se você quiser que a instância spot seja executada em uma zona de disponibilidade de baixo preço, você deve especificar a sub-rede correspondente na solicitação de instância spot. Se você não especificar uma sub-rede, o Amazon EC2 selecionará uma para você, e a zona de disponibilidade para essa sub-rede poderá não ter o menor preço spot.
- [VPC não padrão] Você deve especificar a sub-rede da instância spot.

Histórico de definição de preço da instância spot

Os preços de instâncias spot são definidos pelo Amazon EC2 e ajustados gradualmente de acordo com tendências de longo prazo da oferta e da demanda de capacidade de instâncias spot.

Ao solicitar Instâncias spot, recomendamos que você use o preço máximo padrão (preço sob demanda). Quando sua solicitação for atendida, suas Instâncias spot é lançada pelo preço spot atual, não excedendo o preço sob demanda. Se quiser especificar um preço máximo, é recomendável que você analise antes o histórico de preços spot. Você pode visualizar o histórico de preços spot dos últimos 90 dias, filtrando por tipo de instância, sistema operacional e zona de disponibilidade.

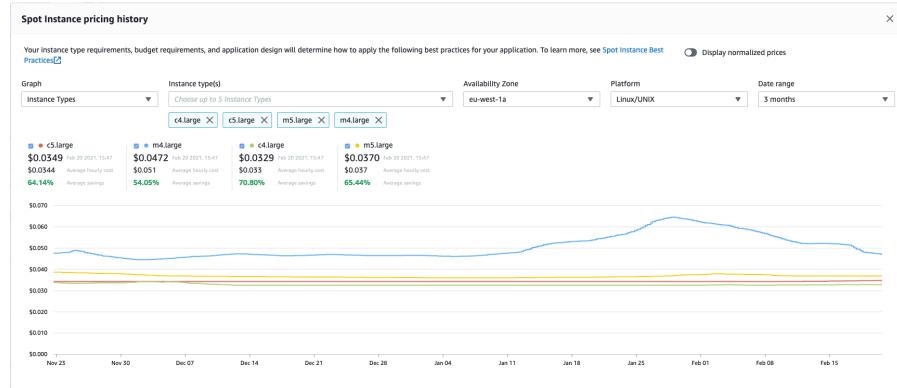
Para exibir os preços spot atuais

Para obter os preços de instâncias spot atuais, consulte a [definição de preço de instâncias spot do Amazon EC2](#).

Para visualizar o histórico de preços spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Escolha Histórico de definição de preço.
4. Em Graph (Gráfico), escolha comparar o histórico de preços por Availability Zones (Zonas de disponibilidade) ou por Instances Types (Tipos de Instância).
 - Se você escolher Availability Zones (Zonas de disponibilidade), escolha o Instance type (Tipo de instância), o sistema operacional (Platform (Plataforma)) e Date range (Intervalo de datas) para o qual exibir o histórico de preços.
 - Se você escolher Instance Types (Tipos de instância), escolha até cinco Instance type(s) (Tipos de instância), a Availability Zone (Zona de disponibilidade), o sistema operacional (Platform (Plataforma)) e o Date range (Intervalo de datas) para os quais exibir o histórico de preços.

A captura de tela a seguir mostra uma comparação de preços para diferentes tipos de instância.



5. Mova o ponteiro do mouse sobre o gráfico para exibir os preços em horas específicas no intervalo de datas selecionado. Os preços são exibidos nos blocos de informações acima do gráfico. O preço exibido na linha superior mostra o preço em uma data específica. O preço exibido na segunda linha mostra o preço médio durante o intervalo de datas selecionado.
6. Para exibir o preço por vCPU, ative a opção Display normalized prices (Exibir preços normalizados). Para exibir o preço do tipo de instância, desative Display normalized prices (Exibir preços normalizados).

Para visualizar o histórico de preços spot usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [describe-spot-price-history](#) (AWS CLI)
- [Get-EC2SpotPriceHistory](#) (AWS Tools for Windows PowerShell)

Economia na compra das Instâncias spot

É possível visualizar as informações de uso e de economias das Instâncias spot em nível de frota ou de todas as Instâncias spot em execução. No nível por frota, as informações de uso e de economia incluem

todas as instâncias executadas e encerradas pela frota. Você pode visualizar essas informações da última hora ou dos últimos três dias.

A captura de tela a seguir da seção Savings (Economia) mostra as informações de uso e de economia spot de uma frota spot.

Spot usage and savings						
4 Spot Instances	266 vCPU-hours	700 Mem(GiB)-hours	\$9.55 On-Demand total	\$2.99 Spot total	69% Savings	
				\$0.0112 Average cost per vCPU-hour	\$0.0043 Average cost per mem(GiB)-hour	
Details						
t3.medium (1)	2 vCPU hours	4 mem(GiB)-hours	\$0.01 total	70% savings		
m4.large (1)	144 vCPU hours	576 mem(GiB)-hours	\$2.52 total	68% savings		
t2.micro (2)	120 vCPU hours	120 mem(GiB)-hours	\$0.46 total	70% savings		

Você pode visualizar as seguintes informações de uso e de economia:

- Spot Instances (Instâncias spot): o número de instâncias spot executadas e encerradas pela frota spot. Ao visualizar o resumo de economias, o número representa todas as Instâncias spot em execução.
- vCPU-hours (Horas de vCPU) – o número de horas de vCPU usadas entre todas as Instâncias spot no período selecionado.
- Mem(GiB)-hours (Horas de mem(GiB)) – o número de horas de GiB usadas entre todas as Instâncias spot no período selecionado.
- On-Demand total (Total sob demanda) – a quantidade total que você pagaria pelo período de tempo selecionado se tivesse executado essas instâncias como Instâncias on-demand.
- Spot total (Total de Spot) – a quantidade total a ser paga para o período selecionado.
- Savings (Economias) – a porcentagem economizada por não pagar o preço sob demanda.
- Average cost per vCPU-hour (Custo médio por hora de vCPU) – o custo médio por hora de uso das vCPUs entre todas as Instâncias spot para o período selecionado, calculado da seguinte forma: Average cost per vCPU-hour (Custo médio por hora de vCPU) = Spot total (Total de Spot) / vCPU-hours (Horas de vCPU).
- Average cost per mem(GiB)-hour (Custo médio por hora de mem(GiB)) – o custo médio por hora de uso de GiBs entre todas as Instâncias spot para o período selecionado, calculado da seguinte forma: Average cost per mem(GiB)-hour (Custo médio por hora de mem(GiB)) = Spot total (Total de Spot) / mem(GiB)-hours (Horas de mem(GiB)).
- Tabela Details (Detalhes): os diferentes tipos de instância (o número de instâncias por tipo de instância está entre parênteses) que compõem a frota spot. Ao visualizar o resumo de economias, isso representa todas as Instâncias spot em execução.

As informações de economias podem ser visualizadas apenas usando o console do Amazon EC2.

Para visualizar as informações de economia de uma frota spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione o ID de uma frota spot e role até seção Savings (Economia).

Se preferir, marque a caixa de seleção ao lado do ID de solicitação de frota spot e escolha a guia seção Savings (Economia).

4. Por padrão, a página exibe as informações de uso e de economia dos últimos três dias. Você pode escolher a last hour (última hora) ou os last three days (últimos três dias). Para Frotas spot que foram executadas há menos de uma hora, a página mostra a economia estimada para a hora.

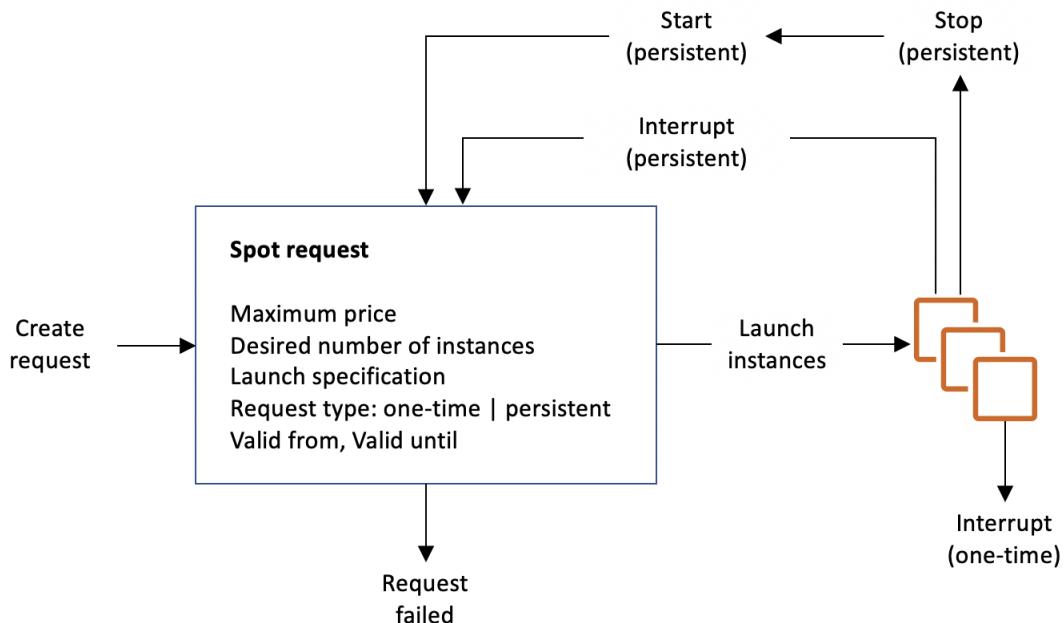
Para visualizar as informações de economias de todas as Instâncias spot em execução (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Escolha Savings Summary (Resumo das economias).

Solicitações de instância Spot

Para usar instâncias spot, você cria uma solicitação de instância spot que inclua o número de instâncias desejado, o tipo de instância, a zona de disponibilidade e o preço máximo que você está disposto a pagar por hora de instância. Se seu preço máximo exceder o preço spot atual, o Amazon EC2 atenderá à sua solicitação imediatamente mediante a disponibilidade de capacidade. Caso contrário, o Amazon EC2 esperará até a sua solicitação puder ser atendida ou até você cancelar a solicitação.

A ilustração a seguir mostra como as solicitações de instância spot funcionam. Observe que o tipo de solicitação (única ou persistente) determina se a solicitação será exibida novamente quando o Amazon EC2 ou você interromper uma instância spot. Se a requisição for persistente, ela será aberta novamente depois que a instância spot for interrompida. Se a solicitação for persistente e você interromper a instância spot, a solicitação será exibida somente depois que você iniciar a instância spot.



Tópicos

- [Estados da solicitação de instância spot \(p. 310\)](#)
- [Definir uma duração para suas Instâncias spot \(p. 311\)](#)
- [Especificar uma locação para suas Instâncias spot \(p. 311\)](#)
- [Função vinculada ao serviço para solicitações de instâncias spot \(p. 311\)](#)

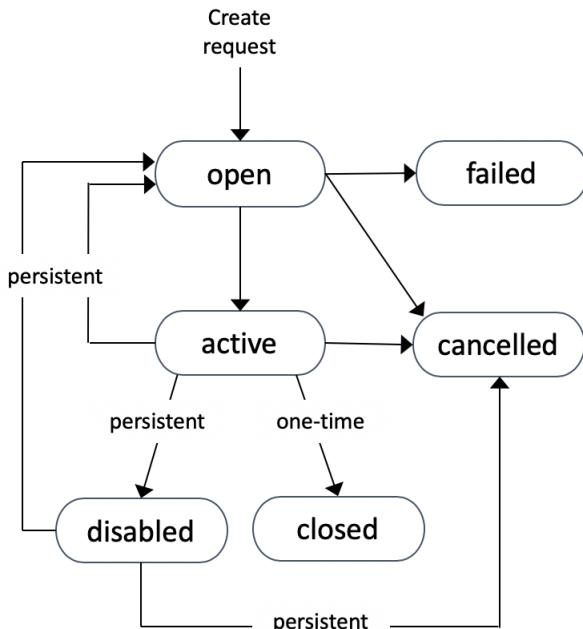
- Criar uma solicitação de instância spot (p. 313)
- Encontrar Instâncias spot em execução (p. 316)
- Marcar solicitações de instância spot (p. 317)
- Cancelar uma solicitação de instância spot (p. 322)
- Interromper uma instância spot (p. 322)
- Iniciar uma instância spot (p. 323)
- Encerrar uma instância spot (p. 324)
- Exemplo de especificações de execução de solicitações de instância spot (p. 325)

Estados da solicitação de instância spot

Uma solicitação de instância spot pode estar em um dos seguintes estados:

- **open**: a solicitação está esperando para ser atendida.
- **active**: a solicitação foi atendida e tem uma instância spot associada.
- **failed**: a solicitação tem um ou mais parâmetros inválidos.
- **closed**: a instância spot foi interrompida ou encerrada.
- **disabled**: você interrompeu a instância spot.
- **cancelled**: você cancelou a solicitação ou ela expirou.

A ilustração a seguir representa as transições entre os estados da solicitação. Observe que as transições dependem do tipo de solicitação (única ou persistente).



Uma solicitação de instância spot única permanece ativa até o Amazon EC2 executar a instância spot, a solicitação expirar ou você cancelar a solicitação. Se o preço spot exceder seu preço máximo ou a capacidade não estiver disponível, sua instância spot será encerrada e a solicitação de instância spot será fechada.

Uma solicitação de instância spot persistente permanecerá ativa até expirar ou até que você a cancele, mesmo se a solicitação tiver sido atendida. Se o preço spot exceder seu preço máximo ou a capacidade

não estiver disponível, sua instância spot será interrompida. Depois que sua instância é interrompida, quando o preço máximo excede o preço spot ou a capacidade se torna disponível novamente, a instância spot será iniciada, se estiver parada, ou retomada, se estiver em hibernação. Você pode interromper uma instância spot e iniciá-la novamente mediante a disponibilidade de capacidade e se o preço máximo exceder o preço spot. Se a instância spot for encerrada (independentemente da instância spot estar interrompida ou estar em execução), a solicitação de instância spot será aberta novamente e o Amazon EC2 executará uma nova instância spot. Para obter mais informações, consulte [Interromper uma instância spot \(p. 322\)](#), [Iniciar uma instância spot \(p. 323\)](#) e [Encerrar uma instância spot \(p. 324\)](#).

Você pode acompanhar o status das solicitações de instância spot, bem como o status das instâncias spot executadas, pelo status. Para obter mais informações, consulte [Status da solicitação spot \(p. 327\)](#).

Definir uma duração para suas Instâncias spot

As instâncias spot com duração definida (também conhecidas como blocos spot) não estarão mais disponíveis para novos clientes a partir de 1º de julho de 2021. Aos clientes que utilizaram o recurso anteriormente, continuaremos a oferecer suporte a instâncias spot com duração definida até 31 de dezembro de 2022.

Especificar uma locação para suas Instâncias spot

Você pode executar uma instância spot no hardware de ocupante único. As instâncias spot dedicadas são fisicamente isoladas de instâncias que pertencem a outras contas da AWS. Para obter mais informações, consulte [Dedicated Instances \(p. 383\)](#) e a página do produto [Instâncias dedicadas do Amazon EC2](#).

Para executar uma instância spot dedicada, execute um dos seguintes procedimentos:

- Especifique um locação `dedicated` ao criar a solicitação de instância spot. Para obter mais informações, consulte [Criar uma solicitação de instância spot \(p. 313\)](#).
- Solicite uma solicitação spot em uma VPC com uma locação de instância `dedicated`. Para obter mais informações, consulte [Criação de uma VPC com uma locação de instância dedicada \(p. 387\)](#). Não é possível solicitar uma instância spot com um locação `default` se você solicitá-la em uma VPC com uma locação de instância `dedicated`.

Todas as famílias de instâncias são compatíveis com Instâncias spot dedicadas, exceto instâncias T. Para cada família de instâncias compatíveis, apenas o maior tamanho de instância ou tamanho de metal é compatível com Instâncias spot dedicadas.

Função vinculada ao serviço para solicitações de instâncias spot

O Amazon EC2 usa funções vinculadas ao serviço para as permissões de que ela precisa para chamar outros produtos da AWS em seu nome. Uma função vinculada ao serviço é um tipo exclusivo de função do IAM que é vinculado diretamente a um produto da AWS. As funções vinculadas a serviços oferecem uma maneira segura de delegar permissões a serviços da AWS, pois somente o serviço vinculado pode assumir uma função vinculada ao serviço. Para obter mais informações, consulte [Uso de funções vinculadas ao serviço](#) no Guia do usuário do IAM.

O Amazon EC2 usa a função vinculada ao serviço denominada `AWSServiceRoleForEC2Spot` para executar e gerenciar Instâncias spot em seu nome.

Permissões concedidas pelo `AWSServiceRoleForEC2Spot`

O Amazon EC2 usa `AWSServiceRoleForEC2Spot` para concluir as ações a seguir:

- `ec2:DescribeInstances`: descrever instâncias spot
- `ec2:StopInstances`: interromper instâncias spot
- `ec2:StartInstances`: iniciar instâncias spot

Criar a função vinculada ao serviço

Na maioria das circunstâncias, você não precisa criar manualmente uma função vinculada ao serviço. O Amazon EC2 cria a função AWSServiceRoleForEC2Spot vinculada ao serviço na primeira vez que você solicita uma instância spot usando o console.

Se você tinha uma solicitação de instância spot ativa antes de outubro de 2017, quando o Amazon EC2 começou a oferecer suporte a essa função vinculada ao serviço, o Amazon EC2 criou a função AWSServiceRoleForEC2Spot em sua conta da AWS. Para obter mais informações, consulte [Uma nova função apareceu na minha conta no Guia do usuário do IAM](#).

Se você usar a AWS CLI ou uma API para solicitar uma instância spot, deverá assegurar que essa função existe.

Para criar um AWSServiceRoleForEC2Spot usando o console

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, selecione Roles.
3. Selecione Create role.
4. Na página Select type of trusted entity (Selecionar tipo de entidade confiável), escolha EC2, EC2 - Spot Instances (EC2 - instâncias spot), Next: Permissions (Próximo: permissões).
5. Na próxima página, escolha Next:Review (Próximo: revisar).
6. Na página Review (Revisar), selecione Create role (Criar função).

Para criar um AWSServiceRoleForEC2Spot usando a AWS CLI

Use o comando [create-service-linked-role](#) da seguinte forma.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Se você não precisar mais usar Instâncias spot, é recomendável excluir a função AWSServiceRoleForEC2Spot. Depois que essa função for excluída da sua conta, o Amazon EC2 criará a função novamente se você solicitar Instâncias spot.

[Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS](#)

Se você especificar uma [AMI criptografada \(p. 135\)](#) ou um [snapshot do Amazon EBS criptografado \(p. 1422\)](#) para suas instâncias spot e usar uma chave gerenciada pelo cliente gerenciada pelo cliente para criptografia, deverá conceder à função AWSServiceRoleForEC2Spot permissão para usar a chave gerenciada pelo cliente de forma que o Amazon EC2 consiga executar instâncias spot em seu nome. Para isso, adicione uma concessão à chave gerenciada pelo cliente, conforme exibido no procedimento a seguir.

Durante a definição de permissões, as concessões são uma alternativa às políticas de chave. Para obter mais informações, consulte [Using grants \(Usar concessões\)](#) e [Using key policies in AWS KMS \(Usar políticas de chave no AWS KMS\)](#) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

Para conceder as permissões para a função AWSServiceRoleForEC2Spot para usar a chave gerenciada pelo cliente

- Use o comando [create-grant](#) para adicionar uma concessão à chave gerenciada pelo cliente e especificar a entidade principal (a função vinculada ao serviço AWSServiceRoleForEC2) que recebe permissão para executar as operações permitidas pela concessão. A chave gerenciada pelo cliente é

especificada pelo parâmetro `key-id` e o ARN da chave gerenciada pelo cliente. A entidade principal é especificada pelo parâmetro `grantee-principal` e pelo ARN da função vinculada ao serviço `AWSServiceRoleForEC2Spot`.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
    east-1:44445556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Spot \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
    "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
    "ReEncryptTo"
```

Criar uma solicitação de instância spot

O procedimento para solicitação de instância spot é semelhante ao procedimento de execução de uma instância sob demanda. Você pode solicitar uma instância spot das seguintes maneiras:

- Para solicitar uma instância spot usando o console, use o assistente de execução de instâncias. Para obter mais informações, consulte [Para criar uma solicitação de instância spot \(console\) \(p. 313\)](#).
- Para solicitar uma instância spot usando a CLI, use o comando `request-spot-instances` ou o comando `run-instances`. Para obter mais informações, consulte [To create a Spot Instance request using request-spot-instances \(CLI\)](#) e [To create a Spot Instance request using run-instances \(CLI\)](#).

Depois de enviar sua solicitação de instância spot, não é possível alterar os parâmetros da solicitação. Isso significa que você não poderá fazer alterações no preço máximo que está disposto a pagar.

Se você solicitar várias instâncias spot ao mesmo tempo, o Amazon EC2 criará solicitações de instância spot separadas para que você possa acompanhar o status de cada uma separadamente. Para obter mais informações sobre como acompanhar solicitações de instâncias spot, consulte [Status da solicitação spot \(p. 327\)](#).

Para executar uma frota que inclui Instâncias spot e Instâncias on-demand, consulte [Criar uma solicitação de frota spot \(p. 776\)](#).

Note

Não é possível executar uma instância spot e uma instância sob demanda na mesma chamada usando o assistente de execução de instância ou o comando `run-instances`.

Prerequisites

Antes de iniciar, decida seu preço máximo, quantas Instâncias spot deseja e qual tipo de instância usar. Para analisar as tendências de preços spot, consulte [Histórico de definição de preço da instância spot \(p. 306\)](#).

Para criar uma solicitação de instância spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação na parte superior da tela, selecione uma região.
3. No painel do console do Amazon EC2, selecione Launch Instance (Executar instância).
4. Na página Escolher imagem de máquina da Amazon (AMI), escolha uma AMI. Para obter mais informações, consulte [Etapa 1: Escolher uma imagem de máquina da Amazon \(AMI\) \(p. 419\)](#).
5. Na página Escolher um tipo de instância, selecione a configuração de hardware e o tamanho da instância a ser executada e Próximo: configurar detalhes da instância. Para obter mais informações, consulte [Etapa 2: escolher um tipo de instância \(p. 420\)](#).

6. Na página Configure Instance Details (Configurar os detalhes da instância) configure a solicitação de instância spot da seguinte maneira:

- Number of instances (Número de instâncias): Digite o número de instâncias para executar.

Note

O Amazon EC2 cria uma solicitação distinta para cada instância spot.

- (Opcional) Para ajudar a assegurar que você mantenha o número de instâncias para lidar com a demanda do aplicativo, escolha Launch into Auto Scaling Group (Executar no grupo de Auto Scaling) para criar uma configuração de execução e um grupo de Auto Scaling. O Auto Scaling escala o número de instâncias no grupo de acordo com suas especificações. Para mais informações, consulte o [Guia do usuário do Amazon EC2 Auto Scaling](#).
- Purchasing option (Opção de compra): escolha Request Spot instances (Solicitar instâncias spot) para executar uma instância Spot. Ao escolher essa opção, os campos a seguir são exibidos.
- Preço atual: o preço spot atual em cada zona de disponibilidade é exibido para o tipo de instância selecionada.
- (Opcional) Preço máximo: você pode deixar o campo vazio ou especificar o valor máximo que está disposto a pagar.
 - Se você deixar o campo vazio, o preço máximo assumirá como padrão o preço sob demanda atual. A instância spot será executada no preço spot atual, não excedendo o preço sob demanda.
 - Se você especificar um preço máximo superior ao preço spot atual, a instância spot será executada e cobrada de acordo com o preço spot atual.
 - Se você especificar um preço máximo inferior ao preço spot, a instância spot não será executada.
- Persistent request (Solicitação persistente): escolha Solicitação persistente para reenviar a solicitação de instância spot se a instância spot for interrompida.
- Interruption behavior (Comportamento de interrupção): por padrão, o serviço spot encerra uma instância spot quando ela é interrompida. Se escolher Solicitação persistente, você poderá especificar que o serviço spot interrompa ou hiberne a instância spot quando ela for interrompida. Para obter mais informações, consulte [Comportamentos de interrupção \(p. 337\)](#).
- (Opcional) Request valid to (Solicitação válida até): escolha Edit (Editar) para especificar a expiração da solicitação de instância spot.

Para obter mais informações sobre como configurar sua instância spot, consulte [Etapa 3: configurar detalhes da instância \(p. 421\)](#).

7. A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume de dispositivo raiz. Na página Add Storage (Adicionar armazenamento), especifique os volumes adicionais para anexar à instância escolhendo Add New Volume (Adicionar novo volume). Para obter mais informações, consulte [Etapa 4: adicionar armazenamento \(p. 423\)](#).
8. Na página Add Tags (Adicionar tags), especifique as [tags \(p. 1554\)](#) fornecendo combinações de chave e valor. Para obter mais informações, consulte [Etapa 5: Adicionar tags \(p. 424\)](#).
9. Na página Configurar grupo de segurança, use um grupo de segurança para definir regras do firewall para sua instância. Essas regras especificam qual tráfego de rede de entrada será fornecido para sua instância. Todo o tráfego é ignorado. (Para mais informações sobre security groups, consulte [Grupos de segurança do Amazon EC2 para instâncias do Windows \(p. 1217\)](#).) Selecione ou crie um grupo de segurança e escolha Revisar e executar. Para obter mais informações, consulte [Etapa 6: configurar o grupo de segurança \(p. 424\)](#).
10. Na página Review Instance Launch (Revisar execução da instância), verifique os detalhes da sua instância e faça qualquer alteração necessária selecionando o link Edit (Editar) apropriado. Quando estiver pronto, escolha Launch (Executar). Para obter mais informações, consulte [Etapa 7: Revisar a execução da instância e selecionar o par de chaves \(p. 425\)](#).
11. Na caixa de diálogo Select an existing key pair or create a new key pair (Selecionar um par de chaves existente ou criar um novo par de chaves), você poderá escolher um par de chaves existente ou

poderá criar um novo. Por exemplo, Escolha um par de chaves existente e selecione o par de chaves que você criou para a configuração. Para obter mais informações, consulte [Pares de chaves do Amazon EC2 e instâncias do Windows \(p. 1209\)](#).

Important

Se você escolher a opção Proceed without key pair (Continuar sem par de chaves), não conseguirá se conectar à instância a menos que escolha uma AMI configurada para permitir aos usuários uma maneira efetuar login.

12. Para executar uma instância, selecione a caixa de confirmação e escolha Launch Instances (Executar instâncias).

Se a instância não executar ou o estado passar imediatamente para terminated, em vez de running, consulte [Solucionar problemas de execução de instâncias \(p. 1570\)](#).

Para criar uma solicitação de instância spot usando [request-spot-instances\(AWS CLI\)](#)

Use o comando [request-spot-instances](#) para criar uma solicitação única:

```
aws ec2 request-spot-instances \
--instance-count 5 \
--type "one-time" \
--launch-specification file://specification.json
```

Use o comando [request-spot-instances](#) para criar uma requisição persistente:

```
aws ec2 request-spot-instances \
--instance-count 5 \
--type "persistent" \
--launch-specification file://specification.json
```

Para que os arquivos de especificação de execução de exemplo sejam usados com esses comandos, consulte [Exemplo de especificações de execução de solicitações de instância spot \(p. 325\)](#). Se você fizer download de um arquivo de especificação de execução no console, use o comando [request-spot-fleet](#) (o console especifica uma solicitação de instância spot usando uma frota spot).

Para criar uma solicitação de instância spot usando [request-spot-instances\(AWS CLI\)](#)

Use o comando [run-instances](#) e especifique as opções da instância spot no parâmetro `--instance-market-options`.

```
aws ec2 run-instances \
--image-id ami-0abcdef1234567890 \
--instance-type t2.micro \
--count 5 \
--subnet-id subnet-08fc749671b2d077c \
--key-name MyKeyPair \
--security-group-ids sg-0b0384b66d7d692f9 \
--instance-market-options file://spot-options.json
```

Veja a seguir a estrutura de dados a ser especificada no arquivo JSON `--instance-market-options`. Também é possível especificar `ValidUntil` e `InstanceInterruptionBehavior`. Se você não especificar um campo na estrutura de dados, será usado o valor padrão. Esse exemplo cria uma solicitação one-time e especifica 0.02 como preço máximo que você está disposto a pagar pela instância spot.

```
{
```

```
"MarketType": "spot",
"SpotOptions": {
    "MaxPrice": "0.02",
    "SpotInstanceType": "one-time"
}
}
```

Encontrar Instâncias spot em execução

O Amazon EC2 executará uma instância spot quando o preço máximo exceder o preço spot e a capacidade estiver disponível. A instância spot será executada até ser interrompida ou até você a encerrar. Se seu preço máximo for exatamente igual ao preço spot, haverá uma possibilidade de a instância spot permanecer em execução, dependendo da demanda.

Para localizar Instâncias spot em execução (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot. Você pode ver solicitações de instância Spot e solicitações de frota spot. Se uma solicitação de instância spot tiver sido atendida, a Capacity (Capacidade) será o ID da instância spot. Em uma frota spot, a Capacity (Capacidade) indica quanto da capacidade solicitada foi atendida. Para exibir os IDs das instâncias em uma frota spot, escolha a seta de expansão ou selecione a frota e escolha Instances (Instâncias).

Note

Para solicitações de instância spot criadas por uma frota spot, as solicitações não são marcadas instantaneamente com a tag do sistema que indica a frota spot a qual pertencem, e por um período podem parecer estarem separadas da solicitação de frota spot.

Como alternativa, no painel de navegação, escolha Instances. No canto superior direito, escolha o ícone (🔍) e em Attribute columns (Colunas de atributo), selecione Instance lifecycle (Ciclo de vida da instância). Para cada instância, o Instance lifecycle (Ciclo de vida da instância) é normal, spot ou scheduled.

Para encontrar instâncias spot em execução (AWS CLI)

Para enumerar as Instâncias spot, use o comando `describe-spot-instance-requests` com a opção `--query`.

```
aws ec2 describe-spot-instance-requests \
--query "SpotInstanceRequests[*].{ID:InstanceId}"
```

A seguir está um exemplo de saída:

```
[  
  {  
    "ID": "i-1234567890abcdef0"  
  },  
  {  
    "ID": "i-0598c7d356eba48d7"  
  }  
]
```

Como alternativa, você pode enumerar as Instâncias spot usando o comando `describe-instances` com a opção `--filters`.

```
aws ec2 describe-instances \
```

```
--filters "Name=instance-lifecycle,Values=spot"
```

Para descrever uma instância spot única, use o comando [describe-spot-instance-requests](#) com a opção `--spot-instance-request-ids`.

```
aws ec2 describe-spot-instance-requests \
--spot-instance-request-ids sir-08b93456
```

Marcar solicitações de instância spot

Para categorizar e gerenciar as solicitações de instância spot, você pode marcá-las com metadados personalizados. Você pode atribuir uma tag a uma solicitação de instância spot ao criá-la ou posteriormente. Você pode atribuir tags usando o console do Amazon EC2 ou uma ferramenta de linha de comando.

Quando você marca uma solicitação de instância spot, as instâncias e os volumes executados pela solicitação de instância spot não são marcados automaticamente. É necessário marcar explicitamente as instâncias e os volumes executados pela solicitação de instância spot. É possível atribuir volumes e uma tag a uma instância spot durante a execução ou posteriormente.

Para obter mais informações sobre como as tags funcionam, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

Tópicos

- [Prerequisites \(p. 317\)](#)
- [Marcar uma nova solicitação de instância spot \(p. 319\)](#)
- [Marcar uma solicitação de instância spot existente \(p. 320\)](#)
- [Exibir tags de solicitação de instância spot \(p. 320\)](#)

Prerequisites

Conceda ao usuário do IAM permissão para marcar recursos. Para obter mais informações sobre políticas do IAM e políticas de exemplo, consulte [Exemplo: marcar recursos \(p. 1178\)](#).

A política do IAM criada é determinada pelo método usado para criação de uma solicitação de instância spot.

- Se você usar o assistente de execução de instâncias ou `run-instances` para solicitar uma Instâncias spot, consulte [To grant an IAM user the permission to tag resources when using the launch instance wizard or run-instances](#).
- Se você utiliza o comando `request-spot-instances` para solicitar instâncias spot, consulte [To grant an IAM user the permission to tag resources when using request-spot-instances](#).

Para conceder a um usuário do IAM permissão para marcar recursos ao usar o assistente de execução ou `run-instances`

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:RunInstances`. Concede ao usuário do IAM permissão para executar uma instância.
- Para `Resource`, especifique `spot-instances-request`. Isso permite que os usuários criem solicitações de instância spot, que solicitam instâncias spot.
- A ação `ec2:CreateTags`. Concede ao usuário do IAM permissão para criar tags.
- Para `Resource`, especifique `*`. Isso permite que os usuários marquem todos os recursos criados durante a execução da instância.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowLaunchInstances",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:us-east-1::image/*",  
                "arn:aws:ec2:us-east-1::subnet/*",  
                "arn:aws:ec2:us-east-1::network-interface/*",  
                "arn:aws:ec2:us-east-1::security-group/*",  
                "arn:aws:ec2:us-east-1::key-pair/*",  
                "arn:aws:ec2:us-east-1::volume/*",  
                "arn:aws:ec2:us-east-1::instance/*",  
                "arn:aws:ec2:us-east-1::spot-instances-request/*"  
            ]  
        },  
        {  
            "Sid": "TagSpotInstanceRequests",  
            "Effect": "Allow",  
            "Action": "ec2:CreateTags",  
            "Resource": "*"  
        }  
    ]  
}
```

Note

Ao usar a ação RunInstances para criar solicitações de instância spot e marcar as solicitações de instância spot na criação, você precisa estar ciente de como o Amazon EC2 avalia o recurso `spot-instances-request` na instrução RunInstances.

O recurso `spot-instances-request` é avaliado na política do IAM da seguinte forma:

- Se você não marcar uma solicitação de instância spot na criação, o Amazon EC2 não avaliará o recurso `spot-instances-request` na instrução RunInstances.
- Se você marcar uma solicitação de instância spot na criação, o Amazon EC2 avaliará o recurso `spot-instances-request` na instrução RunInstances.

Portanto, para o recurso `spot-instances-request`, as seguintes regras se aplicam à diretiva do IAM:

- Caso você use RunInstances para criar uma solicitação de instância spot e não pretenda marcar a solicitação de instância spot na criação, não será necessário permitir explicitamente o recurso `spot-instances-request`. A chamada será bem-sucedida.
- Caso use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, você deverá incluir o recurso `spot-instances-request` na instrução de permissão RunInstances, caso contrário, a chamada falhará.
- Caso você use RunInstances para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, especifique o recurso `spot-instances-request` ou inclua um curinga * na instrução de permissão CreateTags, caso contrário, a chamada falhará.

Por exemplo, políticas do IAM, incluindo políticas que não são compatíveis com solicitações de instância spot, consulte [Trabalhar com Instâncias spot \(p. 1172\)](#).

Para conceder a um usuário do IAM permissão para marcar recursos ao usar `request-spot-instances`

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:RequestSpotInstances`. Concede ao usuário do IAM permissão para criar uma solicitação de instância spot.
- A ação `ec2:CreateTags`. Concede ao usuário do IAM permissão para criar tags.
- Para `Resource`, especifique `spot-instances-request`. Isso permite que os usuários marquem somente a solicitação de instância spot.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "TagSpotInstanceRequest",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RequestSpotInstances",  
                "ec2:CreateTags"  
            ],  
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-request/*"  
        }  
    ]  
}
```

Marcar uma nova solicitação de instância spot

Para marcar uma nova solicitação de instância spot usando o console

1. Siga o procedimento do [Criar uma solicitação de instância spot \(p. 313\)](#).
2. Para adicionar uma tag, na página Adicionar tags, escolha Adicionar tag e insira a chave e o valor da tag. Escolha Adicionar outra tag para cada tag adicional.

Para cada tag, você pode marcar a solicitação de instância spot, as instâncias spot e os volumes com a mesma tag. Para marcar os três, verifique se as opções Instances (Instâncias), Volumes e Spot Instance Requests (Solicitações de instâncias spot) estão selecionadas. Para marcar apenas um ou dois, verifique se os recursos que deseja marcar estão selecionados e os outros recursos estão limpos.

3. Preencha os campos obrigatórios para criar uma solicitação de instância spot e escolha Launch (Executar). Para obter mais informações, consulte [Criar uma solicitação de instância spot \(p. 313\)](#).

Para marcar uma nova solicitação de instância spot usando a AWS CLI

Para marcar uma solicitação de instância spot ao criá-la, defina-a da seguinte maneira:

- Especifique as tags para a solicitação de instância spot usando o parâmetro `--tag-specification`.
- Para `ResourceType`, especifique `spot-instances-request`. Se você especificar outro valor, ocorrerá falha na solicitação de instância spot.
- Em `Tags`, especifique o par de chave/valor. Você pode especificar mais de um par de chave/valor.

No exemplo a seguir, a solicitação de instância spot é marcada com duas tags: `Key=Environment` e `Value=Production`, e `Key=Cost-Center` e `Value=123`.

```
aws ec2 request-spot-instances \  
    --instance-count 5 \  
    --type "one-time" \  
    --launch-specification file://specification.json \  
    --tag-specification 'ResourceType=spot-instances-  
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

Marcar uma solicitação de instância spot existente

Para marcar uma solicitação de instância spot existente usando o console

Depois de criar uma solicitação de instância spot, você pode adicionar tags à solicitação de instância spot usando o console.

1. Abra o console Spot em <https://console.aws.amazon.com/ec2spot>.
2. Selecione sua solicitação de instância spot.
3. Escolha a guia Tags e Create Tag (Criar tag).

Para marcar uma solicitação de instância spot existente usando o console

Depois que sua solicitação de instância spot tiver executado a instância spot, você poderá adicionar tags à instância usando o console. Para obter mais informações, consulte [Adicionar e excluir tags em um recurso individual \(p. 1561\)](#).

Para marcar uma solicitação de instância spot existente ou instância spot usando a AWS CLI

Use o comando [create-tags](#) para marcar os recursos existentes. No exemplo a seguir, a solicitação de instância spot e a instância spot existentes são marcadas com Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources sir-08b93456 i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

Exibir tags de solicitação de instância spot

Para exibir tags de solicitação de instância spot usando o console

1. Abra o console Spot em <https://console.aws.amazon.com/ec2spot>.
2. Selecione sua solicitação de instância spot e escolha a guia Tags.

Para descrever as tags de solicitação de instância spot

Use o comando [describe-tags](#) para exibir as tags para o recurso especificado. No exemplo a seguir, você descreve as tags da solicitação especificada.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sir-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sir-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-instances-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sir-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-instances-request",
            "Value": "Another value"
        }
    ]
}
```

```
}
```

Você também pode exibir as tags de uma solicitação de instância spot descrevendo a solicitação de instância spot.

Use o comando [describe-spot-instance-requests](#) para visualizar a configuração da solicitação de instância spot especificada, que inclui todas as tags especificadas para a solicitação.

```
aws ec2 describe-spot-instance-requests \
--spot-instance-request-ids sir-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
    "SpotInstanceRequests": [
        {
            "CreateTime": "2020-06-24T14:22:11+00:00",
            "InstanceId": "i-1234567890EXAMPLE",
            "LaunchSpecification": {
                "SecurityGroups": [
                    {
                        "GroupName": "launch-wizard-6",
                        "GroupId": "sg-1234567890EXAMPLE"
                    }
                ],
                "BlockDeviceMappings": [
                    {
                        "DeviceName": "/dev/xvda",
                        "Ebs": {
                            "DeleteOnTermination": true,
                            "VolumeSize": 8,
                            "VolumeType": "gp2"
                        }
                    }
                ],
                "ImageId": "ami-1234567890EXAMPLE",
                "InstanceType": "t2.micro",
                "KeyName": "my-key-pair",
                "NetworkInterfaces": [
                    {
                        "DeleteOnTermination": true,
                        "DeviceIndex": 0,
                        "SubnetId": "subnet-11122233"
                    }
                ],
                "Placement": {
                    "AvailabilityZone": "eu-west-1c",
                    "Tenancy": "default"
                },
                "Monitoring": {
                    "Enabled": false
                }
            },
            "LaunchedAvailabilityZone": "eu-west-1c",
            "ProductDescription": "Linux/UNIX",
            "SpotInstanceRequestId": "sir-1234567890EXAMPLE",
            "SpotPrice": "0.012600",
            "State": "active",
            "Status": {
                "Code": "fulfilled",
                "Message": "Your spot request is fulfilled.",
                "UpdateTime": "2020-06-25T18:30:21+00:00"
            },
            "Tags": [
                {

```

```
        "Key": "Environment",
        "Value": "Production"
    },
    {
        "Key": "Another key",
        "Value": "Another value"
    }
],
{
    "Type": "one-time",
    "InstanceInterruptionBehavior": "terminate"
}
]
```

Cancelar uma solicitação de instância spot

Se você não quiser mais sua solicitação de instância spot, poderá cancelá-la. Você só pode cancelar solicitações de instância spot `open`, `active` ou `disabled`.

- A solicitação de instância spot é `open` quando sua requisição não ainda não tiver sido atendida e nenhuma instância tiver sido executada.
- A solicitação de instância spot será `active` quando ela for atendida e as instâncias spot forem executadas como resultado.
- Sua solicitação de instância spot é `disabled` quando você para a instância spot.

Se a solicitação de instância spot estiver `active` e tiver uma instância spot associada em execução, o cancelamento da solicitação não encerrará a instância. Para obter mais informações sobre encerramento de uma instância spot, consulte [Encerrar uma instância spot \(p. 324\)](#).

Para cancelar uma solicitação de instância spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Spot Requests (Solicitações spot) e selecione a solicitação da instância spot.
3. Escolha Ações, Cancelar solicitação.
4. (Opcional) Ao terminar de trabalhar com as Instâncias spot associadas, você poderá encerrá-las. Na caixa de diálogo Cancelar solicitação spot, selecione Encerrar instâncias e escolha Confirmar.

Para cancelar uma solicitação de instância spot (AWS CLI)

- Use o comando `cancel-spot-instance-requests` para cancelar a solicitação de instância spot especificada.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Interromper uma instância spot

Caso você não precise da Instâncias spot agora, mas quiser reiniciá-las posteriormente sem perder os dados persistentes no volume do Amazon EBS, você pode interrompê-los. As etapas para interromper uma instância spot são semelhantes às etapas para interromper uma instância sob demanda.

Note

Quando uma instância spot for interrompida, você poderá modificar alguns atributos da instância, mas não o tipo dela.

Não cobramos pelo uso de uma instância spot interrompida nem por taxas de transferência de dados, mas cobramos pelo armazenamento dos volumes do Amazon EBS.

Limitations

- Você poderá interromper uma instância spot somente se ela tiver sido executada por meio de uma solicitação de instância spot **persistent**.
- Não será possível interromper uma instância spot se a solicitação da instância spot associada for cancelada. Quando a solicitação da instância spot for cancelada, você só poderá terminar a instância spot.
- Não é possível interromper uma instância spot se ela for parte de uma frota ou de um grupo de inicialização ou grupo de zona de disponibilidade.

New console

Para interromper uma instância spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância spot.
3. Escolha Instance state (Estado da instância) e Stop instance (Interromper instância).
4. Quando a confirmação for solicitada, escolha Parar.

Old console

Para interromper uma instância spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância spot.
3. Escolha Ações, Instance State, Parar.

AWS CLI

Para interromper uma instância Spot (AWS CLI)

- Use o comando `stop-instances` para interromper manualmente uma ou mais Instâncias spot.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

Iniciar uma instância spot

É possível iniciar uma instância spot que você encerrou anteriormente. As etapas para iniciar uma instância spot são semelhantes às etapas para iniciar uma instância sob demanda.

Prerequisites

Você pode iniciar uma instância spot somente se:

- Você interrompeu manualmente a instância spot.
- A instância spot é uma instância com EBS.
- A capacidade da instância spot está disponível.
- O preço spot é inferior ao preço máximo.

Limitations

- Não é possível iniciar uma instância spot se ela fizer parte da frota ou do grupo de inicialização ou grupo de zona de disponibilidade.

New console

Para iniciar uma instância Spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância spot.
3. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

Old console

Para iniciar uma instância Spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância spot.
3. Escolha Ações, Estado da instância, Iniciar.

AWS CLI

Para iniciar uma instância spot (AWS CLI)

- Use o comando `start-instances` para iniciar uma ou mais Instâncias spot manualmente.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

Encerrar uma instância spot

Se você terminar uma instância spot em execução ou interrompida que foi executada por uma solicitação de instância spot persistente, a solicitação de instância spot fará a transição para o estado open para que a nova instância spot seja iniciada. Para garantir que nenhuma instância spot nova seja iniciada, primeiro você deve cancelar a solicitação de instância spot.

Se você cancelar uma solicitação de instância spot active com uma instância spot em execução, a instância spot em execução não será automaticamente terminada, e você deverá terminá-la manualmente.

Se você cancelar uma solicitação de instância spot disabled com uma instância spot interrompida, a instância spot interrompida será automaticamente terminada pelo serviço spot do Amazon EC2. Pode haver um pequeno atraso entre o momento em que você cancelar a solicitação de instância spot e o momento em que o serviço spot terminar a instância spot.

Para obter informações sobre como cancelar uma solicitação de instância spot, consulte [Cancelar uma solicitação de instância spot \(p. 322\)](#).

New console

Para encerrar manualmente uma instância spot usando o console

1. Antes de encerrar a instância, confirme que não perderá dados verificando se seus volumes do Amazon EBS não serão excluídos no encerramento e se você copiou todos os dados de que precisa dos volumes de armazenamento persistente de instância, como o Amazon EBS ou o Amazon S3.

2. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
3. No painel de navegação, escolha Instances (Instâncias).
4. Para confirmar se a instância é uma instância spot, verifique se aparece spot na coluna Instance lifecycle (Ciclo de vida da instância).
5. Selecione a instância e escolha Actions (Ações), Instance State (Estado da instância) e Terminate (Encerrar).
6. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Old console

Para encerrar manualmente uma instância spot usando o console

1. Antes de encerrar a instância, confirme que não perderá dados verificando se seus volumes do Amazon EBS não serão excluídos no encerramento e se você copiou todos os dados de que precisa dos volumes de armazenamento persistente de instância, como o Amazon EBS ou o Amazon S3.
2. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
3. No painel de navegação, escolha Instances (Instâncias).
4. Para confirmar se a instância é uma instância spot, verifique se aparece spot na coluna Lifecycle (Ciclo de vida).
5. Selecione a instância e escolha Actions, Instance State e Terminate.
6. Quando a confirmação for solicitada, escolha Sim, encerrar.

AWS CLI

Para encerrar manualmente uma instância spot usando a AWS CLI

- Use o comando `terminate-instances` para encerrar a Instâncias spot manualmente.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

Exemplo de especificações de execução de solicitações de instância spot

Os exemplos a seguir mostram configurações de execução que você pode usar com o comando `request-spot-instances` para criar uma solicitação de instância spot. Para obter mais informações, consulte [Criar uma solicitação de instância spot \(p. 313\)](#).

1. Executar Instâncias spot (p. 325)
2. Executar Instâncias spot na zona de disponibilidade especificada (p. 326)
3. Executar Instâncias spot na sub-rede especificada (p. 326)
4. Executar uma instância spot dedicada (p. 327)

Exemplo 1: Executar Instâncias spot

O exemplo a seguir não inclui uma zona de disponibilidade nem sub-rede. O Amazon EC2 seleciona uma zona de disponibilidade para você. O Amazon EC2 executa as instâncias na sub-rede padrão da zona de disponibilidade selecionada.

```
{  
    "ImageId": "ami-1a2b3c4d",  
    "KeyName": "my-key-pair",  
    "SecurityGroupIds": [ "sg-1a2b3c4d" ],
```

```
"InstanceType": "m3.medium",
"IamInstanceProfile": {
    "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
}
}
```

Exemplo 2: executar Instâncias spot na zona de disponibilidade especificada

O exemplo a seguir inclui uma zona de disponibilidade. O Amazon EC2 executa as instâncias na sub-rede padrão da zona de disponibilidade especificada.

```
{
    "ImageId": "ami-1a2b3c4d",
    "KeyName": "my-key-pair",
    "SecurityGroupIds": [ "sg-1a2b3c4d" ],
    "InstanceType": "m3.medium",
    "Placement": {
        "AvailabilityZone": "us-west-2a"
    },
    "IamInstanceProfile": {
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
    }
}
```

Exemplo 3: executar Instâncias spot na sub-rede especificada

O exemplo a seguir inclui uma sub-rede. O Amazon EC2 executa as instâncias na sub-rede especificada. Se a VPC não for padrão, a instância não receberá um endereço IPv4 público por padrão.

```
{
    "ImageId": "ami-1a2b3c4d",
    "SecurityGroupIds": [ "sg-1a2b3c4d" ],
    "InstanceType": "m3.medium",
    "SubnetId": "subnet-1a2b3c4d",
    "IamInstanceProfile": {
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
    }
}
```

Para atribuir um endereço IPv4 público a uma instância em uma VPC não padrão, especifique o campo `AssociatePublicIpAddress` conforme exibido no seguinte exemplo. Ao especificar uma interface de rede, você deverá incluir o ID da sub-rede e o ID do security group usando a interface de rede, em vez de usar os campos `SubnetId` e `SecurityGroupIds` mostrados no exemplo 3.

```
{
    "ImageId": "ami-1a2b3c4d",
    "KeyName": "my-key-pair",
    "InstanceType": "m3.medium",
    "NetworkInterfaces": [
        {
            "DeviceIndex": 0,
            "SubnetId": "subnet-1a2b3c4d",
            "Groups": [ "sg-1a2b3c4d" ],
            "AssociatePublicIpAddress": true
        }
    ],
    "IamInstanceProfile": {
        "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
    }
}
```

Exemplo 4: executar uma instância spot dedicada

O exemplo a seguir solicita uma instância spot com a locação de `dedicated`. Uma instância spot dedicada deve ser executada em uma VPC.

```
{  
    "ImageId": "ami-1a2b3c4d",  
    "KeyName": "my-key-pair",  
    "SecurityGroupIds": [ "sg-1a2b3c4d" ],  
    "InstanceType": "c3.8xlarge",  
    "SubnetId": "subnet-1a2b3c4d",  
    "Placement": {  
        "Tenancy": "dedicated"  
    }  
}
```

Status da solicitação spot

Para ajudar você a acompanhar suas solicitações de instância spot e planejar o uso de instâncias spot, use o status de solicitação fornecido pelo Amazon EC2. Por exemplo, um status de solicitação informa o motivo por que sua solicitação spot ainda não foi atendida ou lista as restrições que estão impedindo o atendimento de sua solicitação spot.

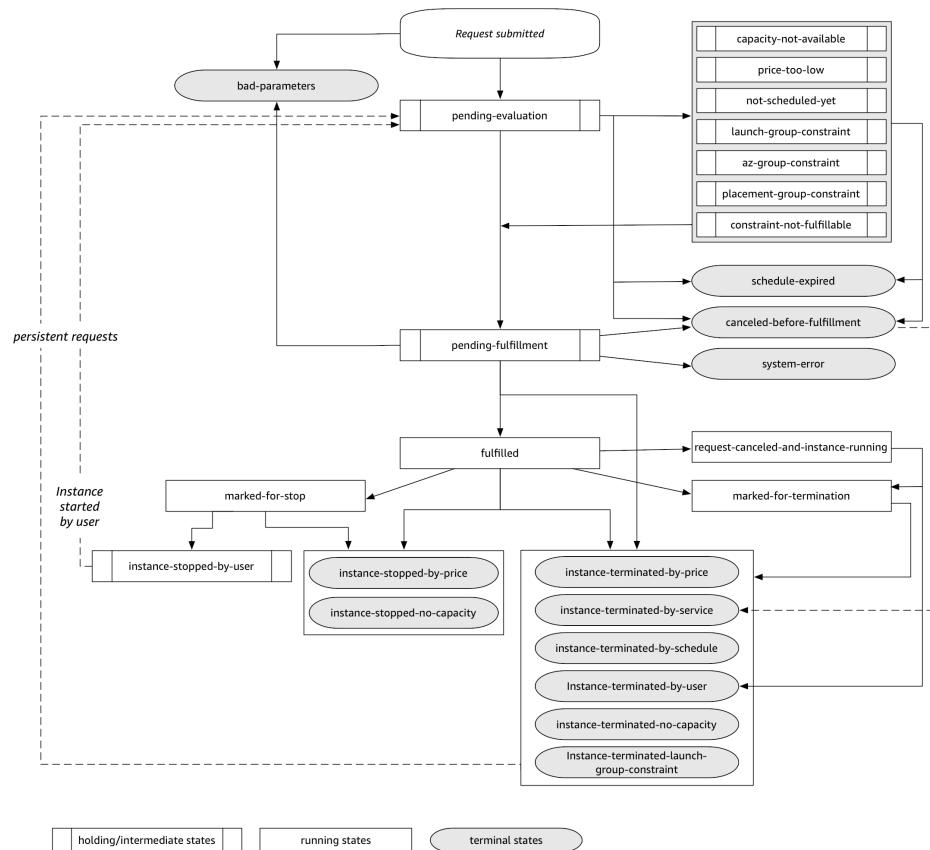
Em cada etapa do processo — também denominado ciclo de vida da solicitação spot — eventos específicos determinam estados sucessivos de solicitação.

Tópicos

- [Ciclo de vida de uma solicitação spot \(p. 327\)](#)
- [Obter informações do status da solicitação \(p. 331\)](#)
- [Códigos de status das solicitações spot \(p. 331\)](#)

Ciclo de vida de uma solicitação spot

O diagrama a seguir mostra os caminhos que a solicitação spot pode seguir durante todo o ciclo de vida, do envio ao encerramento. Cada etapa é representada como um nó, e o código de status de cada nó descreve o status da solicitação spot e da instância spot.



Avaliação pendente

Assim que você cria uma solicitação de instância spot, ela entra no estado **pending-evaluation**, a menos que um ou mais parâmetros da solicitação não sejam válidos (**bad-parameters**).

Código de status	Estado da solicitação	Estado da instância
pending-evaluation	open	n/a
bad-parameters	closed	n/a

Holding

Se uma ou mais restrições da solicitação forem válidas, mas ainda não for possível atendê-las, ou se não houver capacidade suficiente, a solicitação assumirá um estado em espera aguardando que as restrições sejam atendidas. As opções de solicitação afetam a probabilidade de atendimento da solicitação. Por exemplo, se você especificar um preço máximo abaixo do preço spot atual, sua solicitação permanecerá no estado de hibernação até que o preço spot fique abaixo do preço máximo. Se você especificar um grupo de zonas de disponibilidade, a solicitação permanecerá no estado de espera até a restrição de zona de disponibilidade ser atendida.

No caso de interrupção de uma das zonas de disponibilidade, há uma chance de que a capacidade extra do EC2 disponível para solicitações de instância spot em outras zonas de disponibilidade possa ser afetada.

Código de status	Estado da solicitação	Estado da instância
capacity-not-available	open	n/a
price-too-low	open	n/a
not-scheduled-yet	open	n/a
launch-group-constraint	open	n/a
az-group-constraint	open	n/a
placement-group-constraint	open	n/a
constraint-not-fulfillable	open	n/a

Avaliação pendente/atendimento - terminal

A solicitação de instância spot poderá entrar no estado `terminal` se você criar uma solicitação que seja válida somente em um período específico e esse período expirar antes da solicitação atingir a fase de atendimento pendente. Isso também poderá ocorrer se você cancelar a solicitação ou se ocorrer um erro.

Código de status	Estado da solicitação	Estado da instância
schedule-expired	cancelled	n/a
canceled-before-fulfillment*	cancelled	n/a
bad-parameters	failed	n/a
system-error	closed	n/a

* Se você cancelar a solicitação.

Atendimento pendente

Quando as restrições especificadas (se houver) forem atendidas e seu preço máximo for igual ou maior do que o preço spot atual, sua solicitação spot assumirá o estado `pending-fulfillment`.

Nesse momento, o Amazon EC2 está se preparando para provisionar as instâncias solicitadas. Se o processo parar nesse momento, provavelmente foi devido ao seu cancelamento pelo usuário antes da execução de uma instância spot. Isso também pode ocorrer devido a um erro inesperado do sistema.

Código de status	Estado da solicitação	Estado da instância
pending-fulfillment	open	n/a

Fulfilled

Quando todas as especificações das instâncias spot forem atendidas, sua solicitação spot será atendida. O Amazon EC2 executa as instâncias spot, o que pode levar alguns minutos. Se uma instância spot ficar em estado de hibernação, ela permanecerá nesse estado até que a solicitação possa ser atendida novamente ou seja cancelada.

Código de status	Estado da solicitação	Estado da instância
fulfilled	active	pending → running
fulfilled	active	stopped → running

Se você interromper uma instância spot, a solicitação spot entra no estado `marked-for-stop` ou `instance-stopped-by-user` até que a instância spot possa ser iniciada novamente ou até que a solicitação seja cancelada.

Código de status	Estado da solicitação	Estado da instância
<code>marked-for-stop</code>	<code>active</code>	<code>stopping</code>
<code>instance-stopped-by-user</code> *	<code>disabled</code> ou <code>cancelled</code> **	<code>stopped</code>

* Uma instância spot entra no estado `instance-stopped-by-user` se você interromper a instância ou executar o comando de desligamento a partir da instância. Depois de interromper a instância, é possível iniciá-la novamente. Na reinicialização, a solicitação de instância spot retorna para o estado `pending-evaluation` e o Amazon EC2 inicia uma nova instância spot quando as restrições forem atendidas.

** O estado da solicitação spot será `disabled` se você interromper a instância spot, mas não cancelar a solicitação. O estado da solicitação será `cancelled` se a instância spot for interrompida e a solicitação expirar.

Atendido - terminal

As Instâncias spot continuarão em execução, contanto que seu preço máximo seja igual ou superior ao preço spot, haja capacidade disponível para o tipo de instância e você não encerre a instância. Se uma alteração no preço spot ou na capacidade disponível exigir que o Amazon EC2 encerre as Instâncias spot, a solicitação spot entrará no estado terminal. Uma solicitação também entrará no estado terminal se você cancelar a solicitação spot ou encerrar as Instâncias spot.

Código de status	Estado da solicitação	Estado da instância
<code>request-canceled-and-instance-running</code>	<code>cancelled</code>	<code>running</code>
<code>marked-for-stop</code>	<code>active</code>	<code>running</code>
<code>marked-for-termination</code>	<code>active</code>	<code>running</code>
<code>instance-stopped-by-price</code>	<code>disabled</code>	<code>stopped</code>
<code>instance-stopped-by-user</code>	<code>disabled</code>	<code>stopped</code>
<code>instance-stopped-no-capacity</code>	<code>disabled</code>	<code>stopped</code>
<code>instance-terminated-by-price</code>	<code>closed</code> (única), <code>open</code> (persistente)	<code>terminated</code>
<code>instance-terminated-by-schedule</code>	<code>closed</code>	<code>terminated</code>

Código de status	Estado da solicitação	Estado da instância
<code>instance-terminated-by-service</code>	<code>cancelled</code>	<code>terminated</code>
<code>instance-terminated-by-user</code>	<code>closed</code> ou <code>cancelled</code> *	<code>terminated</code>
<code>instance-terminated-no-capacity</code>	<code>closed</code> (única), <code>open</code> (persistente)	<code>terminated</code>
<code>instance-terminated-launch-group-constraint</code>	<code>closed</code> (única), <code>open</code> (persistente)	<code>terminated</code>

* O estado da solicitação será `closed` se você encerrar a instância, mas não cancelar a solicitação. O estado da solicitação será `cancelled` se você encerrar a instância e cancelar a solicitação. Mesmo que você encerre uma instância spot antes de cancelar a solicitação, talvez o Amazon EC2 atrasse a detecção de que a instância spot foi encerrada. Nesse caso, o estado da solicitação poderá ser `closed` ou `cancelled`.

Requisições persistentes

Quando as instâncias spot forem encerradas (por você ou pelo Amazon EC2), se a solicitação spot for uma requisição persistente, ela retornará ao estado `pending-evaluation` e, em seguida, o Amazon EC2 poderá executar uma nova instância spot quando as restrições forem cumpridas.

Obter informações do status da solicitação

Você pode obter informações de status da solicitação usando o AWS Management Console ou a ferramenta de linha de comando.

Para obter informações de status da solicitação (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Spot Requests (Solicitações spot) e selecione a solicitação spot.
3. Para verificar o status, na guia Descrição, marque o campo Status .

Para obter informações de status da solicitação usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- `describe-spot-instance-requests` (AWS CLI)
- `Get-EC2SpotInstanceRequest` (AWS Tools for Windows PowerShell)

Códigos de status das solicitações spot

As informações de status da solicitação spot são compostas de um código de status da solicitação, o tempo de atualização e uma mensagem de status. Juntas, essas informações ajudam a determinar a disposição de sua solicitação spot.

Veja a seguir os códigos de status de solicitação spot:

`az-group-constraint`

O Amazon EC2 não pode executar todas as instâncias que você solicitou na mesma zona de disponibilidade.

bad-parameters

Um ou mais parâmetros para sua solicitação spot são inválidos (por exemplo, a AMI que você especificou não existe). A mensagem de status de solicitação indica qual parâmetro é inválido.

canceled-before-fulfillment

O usuário cancelou a solicitação spot antes de ser atendida.

capacity-not-available

Não há capacidade suficiente disponível para as instâncias solicitadas.

constraint-not-fulfillable

A solicitação spot não pode ser atendida porque uma ou mais restrições são inválidas (por exemplo, a zona de disponibilidade não existe). A mensagem de status de solicitação indica qual restrição é inválida.

fulfilled

A solicitação spot é `active` e Amazon EC2 está executando seu Instâncias spot.

instance-stopped-by-price

Sua instância foi interrompida porque o preço spot excedeu seu preço máximo.

instance-stopped-by-user

A instância foi interrompida porque um usuário interrompeu a instância ou executou o comando de desligamento a partir da instância.

instance-stopped-no-capacity

Sua instância foi interrompida devido às necessidades de gerenciamento de capacidade do EC2.

instance-terminated-by-price

Sua instância foi encerrada porque o preço spot excedeu seu preço máximo. Se sua solicitação for uma sugestão de preço persistente, o processo será reiniciado, portanto, sua solicitação está com a avaliação pendente.

instance-terminated-by-schedule

Sua instância spot foi encerrada no final da duração prevista.

instance-terminated-by-service

A instância foi encerrada em um estado interrompido.

instance-terminated-by-user ou **spot-instance-terminated-by-user**

Você encerrou uma instância spot que tinha sido atendida, portanto, o estado da solicitação é `closed` (a menos que se trate de uma requisição persistente) e o estado da instância é `terminated`.

instance-terminated-launch-group-constraint

Uma ou mais instâncias no grupo de execução foram encerradas, portanto, a restrição do grupo de execução deixou de ser atendida.

instance-terminated-no-capacity

Sua instância foi encerrada devido aos processos padrão de gerenciamento de capacidade.

launch-group-constraint

O Amazon EC2 não pode executar todas as instâncias que você solicitou ao mesmo tempo. Todas as instâncias em um grupo de execução são iniciadas e encerradas juntas.

limit-exceeded

O limite no número de volumes EBS ou de armazenamento de volume total foi excedido. Para obter mais informações sobre esses limites e como solicitar um aumento, consulte [Limites do Amazon EBS](#) no Amazon Web Services General Reference.

marked-for-stop

A instância spot é marcada para interrupção.

marked-for-termination

A instância spot é marcada para encerramento.

not-scheduled-yet

A solicitação spot não é avaliada até a data programada.

pending-evaluation

Após criar uma solicitação de instância spot, ela entrará no estado pending-evaluation enquanto o sistema avalia os parâmetros da solicitação.

pending-fulfillment

O Amazon EC2 está tentando provisionar as Instâncias spot.

placement-group-constraint

A solicitação spot ainda não pode ser atendida porque uma instância spot não pode ser adicionada ao placement group no momento.

price-too-low

A solicitação ainda não pode ser atendida porque seu preço máximo está abaixo do preço spot. Nesse caso, nenhuma instância é executada e sua solicitação permanece open.

request-canceled-and-instance-running

Você cancelou a solicitação spot enquanto as Instâncias spot ainda estão em execução. A solicitação é cancelled, mas instâncias permanecem running.

schedule-expired

A solicitação spot expirou porque não foi atendida antes da data especificada.

system-error

Houve um erro de sistema inesperado. Se esse for um problema recorrente, entre em contato com o AWS Support para obter assistência.

Recomendações de rebalanceamento de instâncias do EC2

Uma recomendação de rebalanceamento de uma instância do EC2 é um sinal que notifica quando uma instância spot tem risco elevado de interrupção. O sinal pode chegar antes do [aviso de interrupção da Instância Spot de dois minutos \(p. 341\)](#), dando a você a oportunidade de gerenciar proativamente a instância spot. Você pode decidir rebalancear sua workload em Instâncias spot novas ou existentes que não tenham risco elevado de interrupção.

Nem sempre é possível para o Amazon EC2 enviar o sinal de recomendação de rebalanceamento antes do aviso de interrupção da Instância spot de dois minutos. Portanto, o sinal de recomendação de rebalanceamento pode chegar junto com o aviso de interrupção de dois minutos.

Note

As recomendações de rebalanceamento só são suportadas para Instâncias spot que sejam executadas depois de 5 de novembro de 2020, 00:00 UTC.

Tópicos

- [Rebalancear ações que você pode executar \(p. 334\)](#)
- [Monitorar os sinais de recomendação de rebalanceamento \(p. 334\)](#)
- [Serviços que usam o sinal de recomendação de rebalanceamento \(p. 336\)](#)

Rebalancear ações que você pode executar

Estas são algumas das possíveis ações de rebalanceamento que você pode executar:

Desligamento normal

Quando você receber o sinal de recomendação de rebalanceamento para uma instância spot, poderá iniciar os procedimentos de desligamento da instância, o que pode incluir a garantia de que os processos sejam concluídos antes de serem interrompidos. Por exemplo, você pode fazer upload de logs de sistema ou de aplicações para o Amazon Simple Storage Service (Amazon S3), desligar operadores do Amazon SQS ou concluir o cancelamento do registro do Sistema de Nomes de Domínio (DNS). Você também pode salvar seu trabalho em armazenamento externo e retomá-lo mais tarde.

Impedir que novos trabalhos sejam programados

Quando você recebe o sinal de recomendação de rebalanceamento para uma instância spot, pode impedir que novos trabalhos sejam programados na instância enquanto ela continuar a ser usada até o trabalho programado ser concluído.

Executar proativamente novas instâncias de substituição

Você pode configurar grupos do Auto Scaling, EC2 Fleet ou frota spot para iniciar automaticamente as instâncias spot de substituição quando um sinal de recomendação de rebalanceamento é emitido. Para obter mais informações, consulte [Amazon EC2 Auto Scaling Capacity Rebalancing \(Rebalanceamento de capacidade do Amazon EC2 Auto Scaling\)](#) no Amazon EC2 Auto Scaling User Guide (Manual do usuário do Amazon EC2 Auto Scaling) e [Rebalanceamento de capacidade \(p. 737\)](#) para EC2 Fleet e [Rebalanceamento de capacidade \(p. 765\)](#) para frota spot neste guia do usuário.

Monitorar os sinais de recomendação de rebalanceamento

Você pode monitorar o sinal de recomendação de rebalanceamento de modo que, quando ele for emitido, você possa executar as ações especificadas na seção anterior. O sinal de recomendação de rebalanceamento é disponibilizado como um evento que é enviado para o Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events) e como metadados de instância na instância spot.

Monitorar sinais de recomendação de rebalanceamento:

- [Usar o Amazon EventBridge \(p. 334\)](#)
- [Usar metadados da instância \(p. 336\)](#)

Usar o Amazon EventBridge

Quando o sinal de recomendação de rebalanceamento é emitido para uma instância spot, o evento para o sinal é enviado para o Amazon EventBridge. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

Veja a seguir um exemplo de evento para o sinal de recomendação de rebalanceamento.

{

```
"version": "0",
"id": "12345678-1234-1234-1234-123456789012",
"detail-type": "EC2 Instance Rebalance Recommendation",
"source": "aws.ec2",
"account": "123456789012",
"time": "yyyy-mm-ddThh:mm:ssZ",
"region": "us-east-2",
"resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
"detail": {
    "instance-id": "i-1234567890abcdef0"
}
}
```

Os campos a seguir formam o padrão de evento definido na regra:

```
"detail-type": "EC2 Instance Rebalance Recommendation"
```

Identifica que o evento é um evento de recomendação de rebalanceamento

```
source": "aws.ec2"
```

Identifica que o evento é de Amazon EC2

Criar uma regra de EventBridge

Você pode escrever uma regra de EventBridge e automatizar quais ações tomar quando o padrão de evento corresponder à regra.

O exemplo a seguir cria uma regra de EventBridge para enviar um e-mail, mensagem de texto ou notificação por push para dispositivos móveis sempre que Amazon EC2 emite um sinal de recomendação de rebalanceamento. O sinal é emitido como um evento de EC2 Instance Rebalance Recommendation, que aciona a ação definida pela regra.

Para criar uma regra de EventBridge para um evento de recomendação de rebalanceamento

1. Abra o console do Amazon EventBridge em <https://console.aws.amazon.com/events/>.
2. Selecione Criar regra.
3. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.

4. Em Define pattern (Definir padrão), selecione Event pattern (Padrão de evento).
5. Em Event matching pattern (Padrão de correspondência de eventos), escolha Custom pattern (Padrão personalizado).
6. Na caixa Event pattern (Padrão de evento), adicione o padrão a seguir para corresponder ao evento de EC2 Instance Rebalance Recommendation e escolha Save (Salvar).

```
{
    "source": [ "aws.ec2" ],
    "detail-type": [ "EC2 Instance Rebalance Recommendation" ]
}
```

7. Em Select event bus (Selecionar barramento de eventos), escolha AWS default event bus (Barramento de eventos padrão da AWS). Quando um serviço da AWS em sua conta emite um evento, ele sempre vai para o barramento de eventos padrão da sua conta.
8. Confirme se Enable the rule on the selected event bus (Habilitar a regra nos barramentos de eventos selecionados) está ativada.
9. Para Target (Destino), escolha SNS topic (tópico SNS) para enviar um e-mail, mensagem de texto ou notificação por push móvel quando o evento ocorrer.

10. Em Topic (Tópico), escolha um tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte [Usar o Amazon SNS para mensagens de aplicação para pessoa \(A2P\)](#) no Guia do desenvolvedor do Amazon Simple Notification Service.
11. Para Configurar entrada, escolha a entrada para e-mail, mensagem de texto ou notificação por push móvel.
12. Escolha Create (Criar).

Para obter mais informações, consulte [Creating a rule for an AWS service \(Criar uma regra para um produto da AWS\)](#) e [Event Patterns \(Padrões de eventos\)](#) no Amazon EventBridge User Guide (Manual do usuário do Amazon EventBridge)

Usar metadados da instância

A categoria de metadados da instância `events/recommendations/rebalance` fornece o horário aproximado, em UTC, quando o sinal de recomendação de rebalanceamento foi emitido para uma Instância spot.

Recomendamos que você verifique se há sinais de recomendação de rebalanceamento a cada 5 segundos para que você não perca a oportunidade de agir de acordo com a recomendação de rebalanceamento.

Se uma instância spot receber uma recomendação de rebalanceamento, o horário em que o sinal foi emitido estará presente nos metadados da instância. Você pode recuperar o horário em que o sinal foi emitido da seguinte forma.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

A seguir, é mostrado um exemplo de saída, que indica o horário, em UTC, em que o sinal de recomendação de rebalanceamento foi emitido para a instância spot.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Se o sinal não tiver sido emitido para a instância, o `events/recommendations/rebalance` não estará presente e você receberá uma mensagem de erro HTTP 404 quando tentar recuperá-lo.

Serviços que usam o sinal de recomendação de rebalanceamento

O Amazon EC2 Auto Scaling, a EC2 Fleet e a frota spot usam o sinal de recomendação de rebalanceamento para facilitar a manutenção da disponibilidade da workload, aumentando proativamente a frota com uma nova instância spot antes que uma instância em execução receba o aviso de interrupção da instância spot de dois minutos. Você pode fazer com que esses serviços monitorem e respondam proativamente às alterações que afetam a disponibilidade das suas Instâncias spot. Para obter mais informações, consulte:

- [Rebalanceamento de capacidade do Amazon EC2 Auto Scaling](#) no Guia do usuário do Amazon EC2 Auto Scaling
- [Rebalanceamento de capacidade \(p. 737\)](#) no tópico Frota do EC2 deste guia do usuário
- [Rebalanceamento de capacidade \(p. 765\)](#) no tópico Frota spot deste guia do usuário

Interrupções de instâncias spot

É possível executar Instâncias spot na capacidade adicional do EC2 para obter grandes descontos em troca de devolvê-los quando o Amazon EC2 precisar da capacidade de volta. Quando o Amazon EC2 recupera uma instância spot, chamamos esse evento de interrupção de instância spot.

A demanda por Instâncias spot pode variar significativamente de um momento para outro, e a disponibilidade das Instâncias spot também pode variar significativamente dependendo de quantas instâncias do EC2 não utilizadas estão disponíveis. É sempre possível que sua instância spot seja interrompida. Portanto, você deve garantir que a aplicação esteja preparada para uma interrupção de instância spot.

Uma instância sob demanda especificada em uma EC2 Fleet ou frota spot não pode ser interrompida.

Tópicos

- [Motivos para interrupção \(p. 337\)](#)
- [Comportamentos de interrupção \(p. 337\)](#)
- [Especificar o comportamento de interrupção \(p. 340\)](#)
- [Preparar-se para interrupções \(p. 340\)](#)
- [Preparar a hibernação de uma instância \(p. 341\)](#)
- [Avisos de interrupção de instância spot \(p. 341\)](#)
- [Encontrar Instâncias spot interrompidas \(p. 343\)](#)
- [Determinar se o Amazon EC2 interrompeu uma instância spot \(p. 343\)](#)
- [Faturamento para Instâncias spot interrompidas \(p. 344\)](#)

Motivos para interrupção

Veja a seguir os possíveis motivos pelos quais o Amazon EC2 pode interromper Instâncias spot:

- Preço: o preço spot é maior do que seu preço máximo.
- Capacidade: o Amazon EC2 pode interromper sua instância spot quando ele precisar dela de volta. O EC2 recupera sua instância principalmente para redirecionar a capacidade, mas também pode ocorrer por outros motivos, como manutenção de host ou descomissionamento de hardware
- Restrições: se a solicitação incluir uma restrição como um grupo de execução ou um grupo de zonas de disponibilidade, essas instâncias spot serão encerradas como um grupo quando não for mais possível atender à restrição.

Você pode ver o histórico de taxas de interrupção para o seu tipo de instância no [Supervisor de instâncias spot](#).

Comportamentos de interrupção

Você pode especificar que o Amazon EC2 deve executar uma das seguintes opções ao interromper uma instância spot:

- [Parar Instâncias spot interrompida \(p. 337\)](#)
- [Hibernar Instâncias spot interrompida \(p. 338\)](#)
- Encerre Instâncias spot interrompidas (este é o comportamento padrão)

Para alterar o comportamento de interrupção, consulte [Especificar o comportamento de interrupção \(p. 340\)](#).

Parar Instâncias spot interrompida

Prerequisites

Você pode especificar o comportamento de interrupção de modo que o Amazon EC2 pare as Instâncias spot quando elas forem interrompidas, se os pré-requisitos a seguir forem cumpridos.

- Tipo de solicitação de instância spot: deve ser `persistent`. Não é possível especificar um grupo de execução na solicitação de instância spot.
- Tipo de solicitação de EC2 Fleet ou frota spot: deve ser `maintain`
- Root volume type (Tipo de volume raiz)– deve ser um volume do EBS, não um volume de armazenamento de instâncias

Depois que uma instância spot é interrompida pelo serviço spot, somente o serviço spot poderá reiniciar a instância spot, e a mesma especificação de execução deverá ser usada.

Para uma instância spot executada por uma solicitação de instância spot `persistent`, o serviço spot reiniciará a instância interrompida quando a capacidade está disponível na mesma zona de disponibilidade e para o mesmo tipo de instância que a instância interrompida.

Se as instâncias de EC2 Fleet e frota spot forem interrompidas e a frota for do tipo `maintain`, o serviço spot executará instâncias de substituição para manter a capacidade desejada. O serviço spot localiza os melhores grupos de capacidade spot com base na estratégia de alocação especificada (`lowestPrice`, `diversified` ou `InstancePoolsToUseCount`); ele não prioriza o grupo com as instâncias interrompidas anteriormente. Posteriormente, se a estratégia de alocação levar a um grupo contendo as instâncias interrompidas anteriormente, o serviço spot reiniciará as instâncias interrompidas para atender à capacidade desejada.

Por exemplo, considere a frota spot com a estratégia de alocação `lowestPrice`. Na execução inicial, um grupo `c3.large` atende aos critérios de `lowestPrice` para a especificação de execução. Posteriormente, quando as instâncias `c3.large` são interrompidas, o serviço spot interrompe as instâncias e repõe a capacidade de outro grupo que se encaixa na estratégia `lowestPrice`. Desta vez, o grupo passa a ser um grupo `c4.large` e o serviço spot executa instâncias `c4.large` para atender a capacidade desejada. Da mesma forma, a frota spot poderia se mover para um grupo `c5.large` da próxima vez. Em cada uma dessas transições, o serviço spot não prioriza grupos com instâncias interrompidas anteriormente, mas prioriza apenas a estratégia de alocação especificada. A estratégia `lowestPrice` pode levar de volta a grupos com instâncias interrompidas anteriormente. Por exemplo, se instâncias forem interrompidas no grupo `c5.large` e a estratégia `lowestPrice` levar de volta aos grupos `c3.large` ou `c4.large`, as instâncias interrompidas anteriormente serão reiniciadas para atender à capacidade de destino.

Quando uma instância spot for interrompida, você poderá modificar alguns atributos da instância, mas não o tipo dela. Se você desanexar ou excluir um volume do EBS, ele não será anexado quando a instância spot for iniciada. Se você desanexar o volume raiz e o serviço spot tentar iniciar a instância spot, a inicialização da instância falhará e o serviço spot encerrará a instância interrompida.

Você pode encerrar uma instância spot enquanto ela está interrompida. Se você cancelar uma solicitação de instância spot, uma EC2 Fleet ou uma frota spot, o serviço spot encerrará todas as instâncias spot associadas que foram interrompidas.

Enquanto uma instância spot estiver interrompida, você será cobrado apenas pelos volumes do EBS, que são preservados. Com a EC2 Fleet e a frota spot, se houver muitas instâncias interrompidas, você poderá exceder o limite de número de volumes do EBS na sua conta.

[Hibernar Instâncias spot interrompida](#)

[Pré-requisitos de hibernação](#)

Você pode especificar o comportamento de interrupção de modo que o Amazon EC2 coloque as Instâncias spot em hibernação quando elas forem interrompidas, se os pré-requisitos a seguir forem cumpridos.

- Tipo de solicitação de instância spot: deve ser `persistent`. Não é possível especificar um grupo de execução na solicitação de instância spot.

- Tipo de solicitação de EC2 Fleet ou frota spot: deve ser `maintain`
- Supported instance families (Famílias de instâncias compatíveis) – C3, C4, C5, M4, M5, R3, R4
- O Instance RAM size (Tamanho de RAM da instância) – deve ser inferior a 100 GB
- Sistemas operacionais com suporte (Você deve instalar o agente de hibernação em um sistema operacional compatível. Como alternativa, use uma AMI compatível, que já inclui o agente.):
 - Amazon Linux 2
 - AMI do Amazon Linux
 - Ubuntu com um kernel Ubuntu ajustado pela AWS (`linux-aws`) maior que 4.4.0-1041
 - Windows Server 2008 R2 e posteriores
- Supported AMIs (AMIs compatíveis) (as AMIs compatíveis a seguir incluem o agente de hibernação):
 - Amazon Linux 2
 - Amazon Linux AMI 2017.09.1 ou posterior
 - Ubuntu Xenial 16.04 20171121 ou versão posterior
 - Windows Server 2008 R2 AMI 2017.11.19 ou versão posterior
 - Windows Server 2012 ou Windows Server 2012 R2 AMI 2017.11.19 ou versão posterior
 - Windows Server 2016 AMI 2017.11.19 ou versão posterior
 - Windows Server 2019
- Root volume type (Tipo do volume da raiz) – deve ser um volume do EBS, e não um volume do armazenamento de instâncias, e deve ser grande o suficiente para armazenar a memória da instância (RAM) durante a hibernação.
- Start the hibernation agent (Iniciar o agente de hibernação) – Recomendamos que você use dados do usuário para iniciar o agente no startup da instância. Se preferir, você pode iniciar o agente manualmente.

Recommendation

- Recomendamos que você use um volume do Amazon EBS criptografado como o volume raiz, porque a memória da instância fica armazenada no volume raiz durante a hibernação. Isso garante que o conteúdo da memória (RAM) permaneça criptografado quando os dados estiverem em repouso no volume e quando forem transmitidos entre a instância e o volume. Use uma das três opções a seguir para garantir que o volume raiz seja um volume criptografado do Amazon EBS:
 - Criptografia do EBS em etapa única: em uma chamada de API de instâncias de execução única, você abre as instâncias do EC2 baseadas em EBS criptografadas a partir de uma AMI não criptografada. Para obter mais informações, consulte [Usar criptografia com AMIs com EBS \(p. 135\)](#).
 - Criptografia do EBS por padrão: você pode habilitar a criptografia do EBS por padrão ao garantir que todos os novos volumes do EBS criados na sua conta da AWS sejam criptografados. Para obter mais informações, consulte [Criptografia por padrão \(p. 1426\)](#).
 - AMI criptografada: você pode habilitar a criptografia do EBS usando uma AMI criptografada para executar sua instância. Se a sua AMI não tiver um snapshot raiz criptografado, você poderá copiá-lo para uma nova AMI e solicitar a criptografia. Para obter mais informações, consulte [Criptografar uma imagem não criptografada durante a cópia \(p. 139\)](#) e [Copiar um AMI \(p. 122\)](#).

Quando uma instância spot é colocada em estado de hibernação pelo serviço spot, os volumes do EBS são preservados e a memória de instância (RAM) é preservada no volume raiz. Os endereços IP privados da instância também são preservados. Volumes do armazenamento de instâncias e endereços IP públicos (que não sejam endereços IP elásticos) não são preservados. Embora a instância esteja hibernando, você é cobrado apenas pelos volumes do EBS. Com a EC2 Fleet e a frota spot, se houver muitas instâncias hibernadas, você poderá exceder o limite de número de volumes do EBS na sua conta.

O agente solicita hibernação ao sistema operacional quando a instância recebe um sinal do serviço spot. Se o agente não estiver instalado, o sistema operacional subjacente não oferecer suporte à hibernação.

ou não houver espaço de volume suficiente para salvar a memória da instância, a hibernação falhará e o serviço spot interromperá a instância.

Quando o serviço spot colocar uma instância spot em hibernação, você receberá um aviso de interrupção, mas não terá dois minutos antes da interrupção da instância spot. A hibernação começa imediatamente. Enquanto a instância estiver em processo de hibernação, as verificações de integridade da instância poderão falhar. Quando o processo de hibernação for concluído, o estado da instância será `stopped`.

Retomar uma instância spot hibernada

Depois que uma instância spot for colocada em estado de hibernação pelo serviço spot, ela só poderá ser retomada pelo serviço spot. O serviço spot retomará a instância quando a houver capacidade disponível com um preço spot inferior ao seu preço máximo especificado.

Para obter mais informações, consulte [Preparar a hibernação de uma instância \(p. 341\)](#).

Para obter informações sobre a hibernação de Instâncias on-demand, consulte [Hibernar a instância do Linux sob demanda ou reservada \(p. 459\)](#).

Especificando o comportamento de interrupção

Se você não especificar um comportamento de interrupção, o padrão será encerrar as Instâncias spot quando elas forem interrompidas. Você pode especificar o comportamento de interrupção ao criar uma solicitação de instância spot. A maneira pela qual você especifica o comportamento de interrupção pode diferir dependendo de como você solicita as Instâncias spot.

Se você solicitar as Instâncias spot usando o [assistente de execução de instância \(p. 419\)](#), poderá especificar o comportamento de interrupção da seguinte maneira: marque a caixa de seleção Requisição persistente e, em Comportamento da interrupção, escolha um comportamento de interrupção.

Se você solicitar as Instâncias spot usando o [console do Spot \(p. 776\)](#), poderá especificar o comportamento de interrupção da seguinte maneira: marque a caixa de seleção Manter capacidade de destino e, em Comportamento de interrupção, escolha um comportamento de interrupção.

Se você configurar as Instâncias spot em um [modelo de execução \(p. 427\)](#), poderá especificar o comportamento de interrupção da seguinte forma: no modelo de execução, expanda Advanced details (Detalhes avançados) e marque a caixa de seleção Request (Solicitar) Instâncias spot. Escolha Personalizar e, em Comportamento de interrupção, escolha um comportamento de interrupção.

Se você configurar as Instâncias spot em uma configuração de execução ao usar a CLI de `request-spot-fleet`, poderá especificar o comportamento de interrupção da seguinte maneira: para `InstanceInterruptionBehavior`, especifique um comportamento de interrupção.

Se você configurar as Instâncias spot usando a CLI de `request-spot-instances`, poderá especificar o comportamento de interrupção da seguinte forma: para `--instance-interruption-behavior`, especifique um comportamento de interrupção.

Preparar-se para interrupções

Veja a seguir algumas práticas recomendadas a serem seguidas durante o uso das Instâncias spot:

- Use o preço máximo padrão, que é o preço sob demanda.
- Certifique-se de que sua instância esteja preparada assim que a solicitação seja atendida usando uma Imagem de máquina da Amazon (AMI) que contenha a configuração de software necessária. Você também pode usar dados de usuário para executar comandos na inicialização.
- Armazene regularmente os dados importantes em um lugar em que eles não sejam afetados quando a instância spot for encerrada. Por exemplo, você pode usar o Amazon S3, o Amazon EBS ou o DynamoDB.
- Divida o trabalho em tarefas pequenas (usando uma grade, um Hadoop ou uma arquitetura baseada em fila) ou use pontos de verificação para que você possa salvar seu trabalho com frequência.

- O Amazon EC2 emite um sinal de recomendação de rebalanceamento para a instância spot quando a instância apresenta risco elevado de interrupção. Você pode confiar na recomendação de rebalanceamento para gerenciar proativamente as interrupções de instância spot sem precisar aguardar o aviso de interrupção de dois minutos da instância spot. Para obter mais informações, consulte [Recomendações de rebalanceamento de instâncias do EC2 \(p. 333\)](#).
- Use os avisos de interrupção de instância spot para monitorar o status das instâncias spot. Para obter mais informações, consulte [Avisos de interrupção de instância spot \(p. 341\)](#).
- Embora nos esforcemos ao máximo para fornecer esse aviso o mais rápido possível, pode ser que a instância spot seja interrompida antes que o aviso seja disponibilizado. Teste sua aplicação para garantir que ele lide tranquilamente com a interrupção inesperada de uma instância, mesmo que você esteja monitorando sinais de recomendação de rebalanceamento e avisos de interrupção. Você pode fazer isso executando a aplicação com uma instância sob demanda e, em seguida, encerrando a instância sob demanda por conta própria.

Preparar a hibernação de uma instância

Você precisa instalar um agente de hibernação na sua instância, a menos que use uma AMI que já inclui o agente. É necessário executar o agente no startup da instância, independentemente de ele ter sido incluído na sua AMI ou instalado por você.

O procedimento a seguir ajuda você a preparar uma instância do Windows. Para obter instruções sobre como preparar uma instância Linux, consulte [Preparar para hibernação de uma instância](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Para preparar uma instância do Windows

1. Se sua AMI não incluir o agente, faça download dos seguintes arquivos na pasta C:\Program Files\Amazon\Hibernate da sua instância do Windows:
 - [EC2HibernateAgent.exe](#)
 - [EC2HibernateAgent.ps1](#)
 - [LICENSE.txt](#)
2. Adicione estes comandos aos dados do usuário.

```
<powershell>."C:\Program Files\Amazon\Hibernate\EC2HibernateAgent.exe"</powershell>
```

Avisos de interrupção de instância spot

A melhor maneira de lidar com interrupções de instâncias spot com tranquilidade é arquitetar a aplicação para que ela seja tolerante a falhas. Para fazer isso, você pode aproveitar os avisos de interrupção de instância spot. Um aviso de interrupção da instância spot é um aviso emitido dois minutos antes de o Amazon EC2 parar ou encerrar uma instância spot. Se você especificar uma hibernação como o comportamento de interrupção, receberá um aviso de interrupção, mas não receberá o aviso dois minutos antes porque o processo de hibernação começará imediatamente.

Recomendamos que você verifique esses avisos de interrupção a cada 5 segundos.

Esses avisos de interrupção são disponibilizados como um evento do CloudWatch e como itens nos [metadados de instância \(p. 622\)](#) na instância spot. Eventos são emitidos com base no melhor esforço.

[EC2 Spot Instance interruption notice](#)

Quando o Amazon EC2 vai interromper a instância spot, ele emite um evento dois minutos antes da interrupção real (exceto para a hibernação, que recebe o aviso de interrupção, mas não dois minutos antes, porque a hibernação começa imediatamente). Esse evento pode ser detectado pelo Amazon

CloudWatch Events. Para obter mais informações sobre as métricas do CloudWatch, consulte o [Amazon CloudWatch Events User Guide \(Manual do usuário do Amazon CloudWatch Events\)](#). Para obter um exemplo detalhado que orienta você sobre como criar e usar regras de evento, consulte [Aproveitar os avisos de interrupção de instância spot do Amazon EC2](#).

Este é um exemplo do evento de interrupção da instância spot. Os valores possíveis para `instance-action` são `hibernate`, `stop` e `terminate`.

```
{  
    "version": "0",  
    "id": "12345678-1234-1234-1234-123456789012",  
    "detail-type": "EC2 Spot Instance Interruption Warning",  
    "source": "aws.ec2",  
    "account": "123456789012",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-2",  
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],  
    "detail": {  
        "instance-id": "i-1234567890abcdef0",  
        "instance-action": "action"  
    }  
}
```

instance-action

Se a instância spot estiver marcada para ser interrompida ou encerrada pelo serviço spot, o item `instance-action` estará presente nos [metadados de instância \(p. 622\)](#). Caso contrário, não estará presente. Você pode recuperar `instance-action` da maneira a seguir.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

O item `instance-action` especifica a ação e o tempo aproximado (em UTC) em que a ação ocorrerá.

O exemplo a seguir indica o momento em que essa instância será interrompida.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

O exemplo a seguir indica o momento em que essa instância será encerrada.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Se o Amazon EC2 não estiver se preparando para interromper ou encerrar a instância, ou se você mesmo encerrar a instância, `instance-action` não estará presente e você receberá um erro HTTP 404 ao tentar recuperá-la.

termination-time

Este item é mantido para compatibilidade com versões anteriores. Você deve usar `instance-action` em seu lugar.

Se a instância spot estiver marcada para encerramento pelo serviço spot, o item `termination-time` estará presente nos metadados de instância. Caso contrário, não estará presente. Você pode recuperar `termination-time` da maneira a seguir.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

O item `termination-time` especifica o tempo aproximado (em UTC) em que a instância recebe o sinal de desligamento. Por exemplo:

```
2015-01-05T18:02:00Z
```

Se o Amazon EC2 não estiver se preparando para encerrar a instância ou se você tiver encerrado a instância spot por conta própria, o item `termination-time` não estará presente (e você receberá um erro HTTP 404) ou conterá um valor que não é um valor de tempo.

Se o Amazon EC2 não encerrar a instância, o status da solicitação será definido como `fulfilled`. O valor de `termination-time` permanece nos metadados da instância com o tempo aproximado original, que agora está no passado.

Encontrar Instâncias spot interrompidas

No console, o painel Instâncias exibe todas as instâncias, inclusive Instâncias spot. Você pode identificar uma instância spot usando o valor de `spot` na coluna `Instance lifecycle` (Ciclo de vida da instância). A coluna `Instance state` (Estado da instância) indica se a instância está `pending`, `running`, `stopping`, `stopped`, `shutting-down` ou `terminated`. Para uma instância spot hibernada, o estado da instância é `stopped`.

Para encontrar uma instância spot interrompida (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias). No canto superior direito, selecione o ícone  de configurações e em Attribute columns (Colunas de atributo), selecione Instance lifecycle (Ciclo de vida da instância). Em Instâncias spot, o Instance lifecycle (Ciclo de vida da instância) é spot.
Como alternativa, no painel de navegação, escolha Solicitações spot. Você pode ver solicitações de instância Spot e solicitações de frota spot. Para exibir as IDs das instâncias, selecione uma solicitação de instância spot ou uma solicitação de frota spot e escolha a aba Instances (Instâncias). Escolha um ID de instância para exibir a instância no painel Instâncias.
3. Para cada instância spot, você pode exibir o estado na coluna `Instance State` (Estado da instância).

Para encontrar instâncias spot interrompidas (AWS CLI)

Você pode listar as Instâncias spot interrompidas usando o comando `describe-instances` com o parâmetro `--filters`. Para listar apenas os IDs das instâncias na saída, adicione o parâmetro `--query`.

```
aws ec2 describe-instances \
--filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=terminated,stopped \
--query "Reservations[*].Instances[*].InstanceId"
```

Determinar se o Amazon EC2 interrompeu uma instância spot

Se uma instância spot for interrompida, hibernada ou encerrada, você pode usar o CloudTrail para ver se o Amazon EC2 interrompeu a instância spot. Em AWS CloudTrail, o nome do evento `BidEvictedEvent` indica que o Amazon EC2 interrompeu a instância spot.

Para exibir eventos `BidEvictedEvent` no CloudTrail

1. Abra o console do CloudTrail em <https://console.aws.amazon.com/cloudfront/>.
2. No painel de navegação, selecione Event history (Histórico de eventos).

3. No menu suspenso de filtros, escolha Event name (Nome do evento) e, em seguida, no campo de filtro à direita, digite BidEvictedEvent.
4. Selecione BidEvictedEvent na lista resultante e você poderá visualizar seus detalhes. Em Event record (Registro de evento), você pode encontrar o ID da instância.

Para obter mais informações sobre o uso de CloudTrail, consulte [Registrar em log o Amazon EC2 e chamadas de APIs do Amazon EBS com o AWS CloudTrail \(p. 937\)](#).

Faturamento para Instâncias spot interrompidas

Quando uma instância spot é interrompida, você é cobrado da maneira indicada a seguir.

Quem interrompe a instância spot	Sistema operacional	Interrompida na primeira hora	Interrompida em qualquer hora após a primeira
Se você interromper ou encerrar a instância spot	Windows e Linux (com exceção de RHEL e SUSE)	Cobrança pelos segundos usados	Cobrança pelos segundos usados
	RHEL e SUSE	Cobrança pela hora completa, mesmo se você usou somente uma parte da hora	Cobrança pelas horas completas usadas e cobrança por uma hora completa pela hora parcial interrompida
Se o serviço spot do Amazon EC2 interromper a instância spot	Windows e Linux (com exceção de RHEL e SUSE)	Sem cobrança	Cobrança pelos segundos usados
	RHEL e SUSE	Sem cobrança	Cobrança pelas horas completas usadas, mas sem cobrança pela hora parcial interrompida

Feed de dados da instância spot

Para compreender as cobranças relativas às suas instâncias spot, o Amazon EC2 fornece um feed de dados que descreve o uso que você faz de sua instância spot e a definição de preços. Esse feed de dados é enviado a um bucket do Amazon S3 que você especifica ao assinar um feed de dados.

O feed de dados chega em seu bucket geralmente uma vez por hora, e cada hora de uso geralmente é coberto em um único arquivo de dados. Esses arquivos são compactados (gzip) antes de serem entregues ao seu bucket. O Amazon EC2 pode gravar vários arquivos em uma determinada hora de uso quando os arquivos estiverem muito grandes (por exemplo, quando o conteúdo dos arquivos para a hora ultrapassar 50 MB antes da compactação).

Note

Se você não tiver uma instância spot em execução em uma hora específica, não receberá um arquivo de feed de dados nessa hora.

O feed de dados da instância spot é compatível em todas as Regiões AWS, exceto China (Pequim), China (Ningxia), AWS GovCloud (EUA) e as [Regiões que estão desabilitadas por padrão](#).

Tópicos

- [Nome e formato de arquivo do feed de dados \(p. 345\)](#)
- [Requisitos do bucket do Amazon S3 \(p. 345\)](#)
- [Assinar seu feed de dados da instância spot \(p. 346\)](#)
- [Descrever seu feed de dados de instância spot \(p. 346\)](#)
- [Excluir seu feed de dados de instância spot \(p. 347\)](#)

Nome e formato de arquivo do feed de dados

O nome de arquivo do feed de dados de instância spot usa o seguinte formato (com a data e a hora em UTC):

`bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz`

Por exemplo, se o nome do bucket for **my-bucket-name** e o prefixo for **my-prefix**, os nomes dos arquivos serão semelhantes ao seguinte:

`my-bucket-name.s3.amazonaws.com/my-prefix/111122223333.2019-03-17-20.001.pwBdGTJG.gz`

Para obter mais informações sobre os nomes de bucket, consulte [Regras para nomeação de bucket](#) no Guia do desenvolvedor do Amazon Simple Storage Service.

Os arquivos de feed de dados de instância spot são delimitados por tabulação. Cada linha no arquivo de dados corresponde a uma hora de instância e contém os campos listados na tabela a seguir.

Campo	Descrição
<code>Timestamp</code>	O time stamp usado para determinar o preço cobrado pelo uso dessa instância.
<code>UsageType</code>	O tipo de uso e instância que está sendo cobrado. Para <code>m1.small</code> Instâncias spot, este campo está definido como <code>SpotUsage</code> . Para todos os outros tipos de instância, esse campo é definido como <code>SpotUsage:{instance-type}</code> . Por exemplo, <code>SpotUsage:c1.medium</code> .
<code>Operation</code>	O produto que está sendo cobrado. Nas Instâncias spot do Linux, este campo é definido como <code>RunInstances</code> . Nas Instâncias spot do Windows, este campo é definido como <code>RunInstances:0002</code> . O uso de spot é agrupado de acordo com a zona de disponibilidade.
<code>InstanceId</code>	O ID da instância spot que gerou este uso de instância.
<code>MyBidID</code>	O ID da solicitação de instância spot que gerou este uso de instância.
<code>MyMaxPrice</code>	O preço máximo especificado para essa solicitação de instância spot.
<code>MarketPrice</code>	O preço spot na hora especificada no campo <code>Timestamp</code> .
<code>Charge</code>	O preço cobrado por este uso de instância.
<code>Version</code>	A versão incluída no nome do arquivo de feed de dados para esse registro.

Requisitos do bucket do Amazon S3

Ao assinar o feed de dados, você deve especificar um bucket do Amazon S3 pra armazenar os arquivos do feed de dados. Antes de escolher um bucket do Amazon S3 para o feed de dados, considere o seguinte:

- Você deve ter a permissão **FULL_CONTROL** para o bucket, incluindo permissão para as ações **s3:GetBucketAcl** e **s3:PutBucketAcl**.

Se você for o proprietário do bucket, terá essa permissão por padrão. Caso contrário, o proprietário do bucket deve conceder essa permissão à sua conta da AWS.

- Quando você assina um feed de dados, essas permissões são usadas para atualizar o ACL do bucket a fim de fornecer permissão à AWS conta de feed de dados da **FULL_CONTROL**. A conta de feed de dados da AWS grava arquivos de feed de dados no bucket. Se sua conta não tiver as permissões necessárias, os arquivos de feed de dados não poderão ser gravados no bucket.

Note

Se você atualizar o ACL e eliminar as permissões para a conta do feed de dados da AWS, os arquivos de feed de dados não poderão ser gravados no bucket. Você deve assinar novamente o feed de dados para receber arquivos de feed de dados.

- Cada arquivo do feed de dados tem sua própria ACL (separada da ACL do bucket). O proprietário do bucket tem a permissão **FULL_CONTROL** para os arquivos de dados. A conta de feed de dados da AWS tem permissões de leitura e gravação.
- Se você excluir a assinatura do feed de dados, o Amazon EC2 não removerá as permissões de leitura e gravação para a conta de feed de dados da AWS no bucket, nem nos arquivos de dados. Você precisa remover essas permissões por conta própria.

Assinar seu feed de dados da instância spot

Para assinar o feed de dados, use o comando [create-spot-datafeed-subscription](#).

```
aws ec2 create-spot-datafeed-subscription \
--bucket my-bucket-name \
[--prefix my-prefix]
```

A seguir está um exemplo de saída:

```
{  
    "SpotDatafeedSubscription": {  
        "OwnerId": "111122223333",  
        "Bucket": "my-bucket-name",  
        "Prefix": "my-prefix",  
        "State": "Active"  
    }  
}
```

Descrever seu feed de dados de instância spot

Para descrever sua assinatura do feed de dados, use o comando [describe-spot-datafeed-subscription](#).

```
aws ec2 describe-spot-datafeed-subscription
```

A seguir está um exemplo de saída:

```
{  
    "SpotDatafeedSubscription": {  
        "OwnerId": "123456789012",  
        "Prefix": "spotdata",  
        "Bucket": "my-s3-bucket",  
        "State": "Active"  
    }  
}
```

}

Excluir seu feed de dados de instância spot

Para excluir o feed de dados, use o comando [delete-spot-datafeed-subscription](#).

```
aws ec2 delete-spot-datafeed-subscription
```

Limites de instância spot

Há um limite para o número de instâncias spot em execução e solicitadas por conta da AWS por Região. Os limites de instância spot são gerenciados em termos do número de unidades de processamento central virtuais (vCPUs) que as instâncias spot em execução estão usando ou usarão até o atendimento de solicitações de instância spot abertas. Se você encerrar as instâncias spot, mas não cancelar as solicitações de instância spot, as solicitações serão contabilizadas em relação ao limite de vCPU da instância spot até que o Amazon EC2 detecte os encerramentos de instância spot e feche as solicitações.

Há seis limites de instância spot:

- Todas as solicitações de instância spot padrão (A, C, D, H, I, M, R, T, Z)
- Todas as solicitações de instância spot F
- Todas as solicitações de instância spot G
- Todas as solicitações de instância spot Inf
- Todas as solicitações de instância spot P
- Todas as solicitações de instância spot X

Cada limite especifica o limite de vCPU para uma ou mais famílias de instâncias. Para obter informações sobre as diferentes famílias, gerações e tamanhos de instâncias, consulte [Tipos de instância do Amazon EC2](#).

Com limites de vCPU, é possível usar seu limite em termos do número de vCPUs necessárias para executar qualquer combinação de tipos de instância que atenda às necessidades em constante mudança da sua aplicação. Por exemplo, se o limite de todas as suas solicitações padrão de instância spot for de 256 vCPUs, você pode solicitar 32 instâncias spot `m5.2xlarge` (32 x 8 vCPUs) ou 16 instâncias spot `c5.4xlarge` (16 x 16 vCPUs) ou uma combinação de quaisquer tipos e tamanhos padrão de instâncias spot que totalizem 256 vCPUs.

Tópicos

- [Monitorar limites e uso de instâncias spot \(p. 347\)](#)
- [Solicitar um aumento de limite de instância spot \(p. 348\)](#)

Monitorar limites e uso de instâncias spot

É possível visualizar e gerenciar seus limites de instância spot usando o seguinte:

- A [página Limites](#) no console do Amazon EC2
- A [página Cotas de serviços](#) do Amazon EC2 no console de Cotas de serviços
- O `get-service-quota` da AWS CLI

Para obter mais informações, consulte [Cotas de serviço do Amazon EC2 \(p. 1567\)](#) no Amazon EC2 User Guide for Linux Instances (Manual do usuário do Amazon EC2 para instâncias do Linux) e [Viewing](#)

[a Service Quota \(Visualizar uma cota de serviço\)](#) no Service Quotas User Guide (Manual do usuário do Service Quotas).

Com a integração de métricas do Amazon CloudWatch, é possível monitorar o uso do EC2 em comparação aos limites. Também é possível configurar alarmes para alertar quando estiver chegando próximo ao limite. Para obter mais informações, consulte [Usar alarmes do Amazon CloudWatch](#) no Guia do usuário de cotas de serviço.

Solicitar um aumento de limite de instância spot

Mesmo que o Amazon EC2 aumente automaticamente seus limites de instância spot com base em seu uso, é possível solicitar um aumento de limite se necessário. Por exemplo, se você pretende lançar mais Instâncias spot do que o limite atual permite, solicite um aumento de limite. Também é possível solicitar um aumento de limite se você enviar uma solicitação de instância spot e receber uma mensagem de erro `Max spot instance count exceeded`.

Para solicitar um aumento de limite de instância spot

1. Abra o formulário Create case (Criar caso), Service limit increase (Aumento do limite de serviço) no console do Support Center em <https://console.aws.amazon.com/support/home#/case/create>.
2. Em Limit type (Tipo de limite), selecione EC2 Spot Instances (Instâncias spot do EC2).
3. Em Region (Região), selecione a região necessária.
4. Em Primary instance type (Tipo de instância principal), selecione o limite de instância spot para o qual você deseja solicitar um aumento.
5. Em New limit value (Novo valor limite), insira o número total de vCPUs que você deseja executar simultaneamente. Para determinar o número total de vCPUs necessárias, consulte [Amazon EC2 Instance Types \(Tipos de instância do Amazon EC2\)](#) para localizar o número de vCPUs de cada tipo de instância.
6. (Condisional) Você deve criar uma solicitação de limite separada para cada limite de instância spot. Para solicitar um aumento para outro limite de instância spot, escolha Add another request (Adicionar outra solicitação) e repita as etapas 4 e 5 deste procedimento.
7. Em Use case description (Descrição de caso de uso), insira o caso de uso e selecione Submit (Enviar).

Para obter mais informações sobre como visualizar os limites e solicitar um aumento de limite, consulte [Cotas de serviço do Amazon EC2 \(p. 1567\)](#).

Instâncias expansíveis

Se você executar as instâncias spot usando um [tipo de instância expansível \(p. 169\)](#) e planeja usar as instâncias spot de performance intermitente imediatamente e por um breve período, sem tempo ocioso para acumular créditos de CPU, recomendamos executá-las no [modo padrão \(p. 185\)](#) para evitar pagar custos mais elevados. Se executar as instâncias spot expansíveis no [modo ilimitado \(p. 177\)](#) e esgotar a CPU imediatamente, você gastará os créditos excedentes por isso. Se a instância for usada por um curto período, não haverá tempo para acumular créditos de CPU para pagamento dos créditos excedentes, e você precisará pagar os créditos excedentes ao encerrar a instância.

O modo ilimitado será adequado para instâncias spot expansíveis somente se a instância for executada por tempo suficiente para acumular créditos de CPU para intermitência. Caso contrário, pagar por créditos excedentes torna as instâncias spot expansíveis mais caras do que o uso de outras instâncias. Para obter mais informações, consulte [Quando usar o modo ilimitado versus CPU fixa \(p. 179\)](#).

Os créditos de lançamento são feitos para fornecer uma experiência de lançamento inicial produtiva para instâncias T2 fornecendo recursos computacionais suficientes para configurar a instância. Lançamentos

repetidos de instâncias T2 para acessar novos créditos de lançamento não são permitidos. Se você precisar de uma CPU sustentada, poderá obter créditos (ficando inativo durante um período), usar o modo Ilimitado (p. 177) para T2 Instâncias spot ou usar um tipo de instância com CPU dedicada.

Dedicated Hosts

Um host dedicado do Amazon EC2 é um servidor físico com capacidade de instância totalmente dedicado para seu uso. Os hosts dedicados permitem que você use suas licenças de software existentes por soquete, por núcleo ou por VM, incluindo o Windows Server, o Microsoft SQL Server, o SUSE e o Linux Enterprise Server.

Para obter informações sobre as configurações compatíveis com os Hosts dedicados, consulte a [Dedicated Hosts Configuration](#) (Configuração de hosts dedicados).

Tópicos

- [Diferenças entre Hosts dedicados e Instâncias dedicadas \(p. 349\)](#)
- [Traga sua própria licença \(p. 350\)](#)
- [Capacidade da instância do Host dedicado \(p. 350\)](#)
- [Instâncias T3 intermitentes em hosts dedicados \(p. 351\)](#)
- [Restrições do Hosts dedicados \(p. 352\)](#)
- [Definição de preço e faturamento \(p. 353\)](#)
- [Como trabalhar com o Hosts dedicados \(p. 354\)](#)
- [Trabalhar com Hosts dedicados compartilhado \(p. 373\)](#)
- [Recuperação do host \(p. 378\)](#)
- [Monitorar alterações de configuração \(p. 382\)](#)

Diferenças entre Hosts dedicados e Instâncias dedicadas

Hosts dedicados e Instâncias dedicadas podem ser usados para executar instâncias do Amazon EC2 em servidores físicos que são dedicados para seu uso.

Não há diferenças físicas de performance ou de segurança entre Instâncias dedicadas e instâncias em Hosts dedicados. No entanto, existem algumas diferenças entre os dois. A tabela a seguir destaca algumas das principais diferenças entre Hosts dedicados e Instâncias dedicadas:

	Dedicated Host	Dedicated Instance
Faturamento	faturamento por host	Faturamento por instância
Visibilidade de soquetes, núcleos e ID de host	Fornece visibilidade do número de soquetes e núcleos físicos	Sem visibilidade
Afinidade de hosts e instâncias	permite implantar de forma consistente suas instâncias no mesmo servidor físico com o momento	Não suportado
Posicionamento direcionado de instâncias	Proporciona visibilidade e controle adicionais sobre como as instâncias são colocadas em um servidor físico	Não suportado

	Dedicated Host	Dedicated Instance
Recuperação automática de instâncias	Compatível. Para obter mais informações, consulte Recuperação do host (p. 378) .	Compatível
Traga sua própria licença (BYOL)	Compatível	Não suportado

Traga sua própria licença

O Hosts dedicados permite usar suas licenças de software por VM, por núcleo e por soquete existentes. Quando você leva sua própria licença, é responsável por gerenciar as próprias licenças. No entanto, o Amazon EC2 tem recursos que ajudam você a manter a conformidade com a licença, como afinidade de instâncias e posicionamento direcionado.

Estas são as etapas gerais para trazer sua própria imagem de máquina com licença por volume para o Amazon EC2.

1. Verifique se os termos de licença que regem o uso de suas imagens de máquina permitem o uso de um ambiente de nuvem virtualizado. Para obter mais informações sobre o Licenciamento da Microsoft, consulte [Amazon Web Services e Licenciamento da Microsoft](#).
2. Depois de verificar se sua imagem de máquina pode ser usada no Amazon EC2, importe-a com o VM Import/Export. Para obter informações sobre como importar sua imagem de máquina, consulte o [Manual do usuário do VM Import/Export](#).
3. Depois de importar a imagem de máquina, você poderá executar instâncias dela no Hosts dedicados ativo na sua conta.
4. Ao executar essas instâncias, dependendo do sistema operacional, talvez seja necessário ativar essas instâncias em seu próprio servidor KMS (por exemplo, Windows Server ou Windows SQL Server). Não é possível ativar a AMI do Windows importada no servidor Amazon Windows KMS.

Note

Para controlar como as imagens são usadas na AWS, ative a gravação de host no AWS Config. Você pode usar o AWS Config para gravar alterações de configuração em um host dedicado e usar a saída como fonte de dados para geração de relatórios de licenças. Para obter mais informações, consulte [Monitorar alterações de configuração \(p. 382\)](#).

Capacidade da instância do Host dedicado

A compatibilidade com vários tamanhos de instância no mesmo Host Dedicado está disponível para as seguintes famílias de instâncias: T3, A1, C5, M5, R5, C5n, R5n e M5n. Outras famílias de instâncias oferecem suporte apenas a um único tamanho de instância no mesmo Host dedicado.

Por exemplo, quando você aloca um R5 Host dedicado, ele possui 2 soquetes e 48 núcleos físicos em que você pode executar diferentes tamanhos de instância, como `r5.2xlarge` e `r5.4xlarge`, até a capacidade de núcleo associada ao host. No entanto, para cada família de instâncias, há um limite no número de instâncias que podem ser executadas para cada tamanho de instância. Por exemplo, um R5 Host dedicado oferece suporte a até 2 instâncias `r5.8xlarge`, que usam 32 dos núcleos físicos. Instâncias R5 adicionais de outro tamanho podem ser usadas para preencher o host até a capacidade de núcleo. Para obter o número compatível de tamanhos de instância para cada família de instâncias, consulte a [Dedicated Hosts Configuration](#) (Configuração de hosts dedicados).

A tabela a seguir mostra exemplos de diferentes combinações de tamanhos de instância que você pode executar em um Host dedicado.

Família de instâncias	Combinações de exemplo de tamanhos de instância
R5	<ul style="list-style-type: none">Exemplo 1: 4 x r5.4xlarge + 4 x r5.2xlargeExemplo 2: 1 x r5.12xlarge + 1 x r5.4xlarge + 1 x r5.2xlarge + 5 x r5.xlarge + 2 x r5.large
C5	<ul style="list-style-type: none">Exemplo 1: 1 x c5.9xlarge + 2 x c5.4xlarge + 1 x c5.xlargeExemplo 2: 4 x c5.4xlarge + 1 x c5.xlarge + 2 x c5.large
M5	<ul style="list-style-type: none">Exemplo 1: 4 x m5.4xlarge + 4 x m5.2xlargeExemplo 2: 1 x m5.12xlarge + 1 x m5.4xlarge + 1 x m5.2xlarge + 5 x m5.xlarge + 2 x m5.large

Para obter mais informações sobre as famílias de instâncias e as configurações de tamanhos de instância compatíveis com o Hosts dedicados, consulte a [Dedicated Hosts Configuration Table](#) (Tabela de configuração de hosts dedicados).

Instâncias T3 intermitentes em hosts dedicados

Hosts dedicados são compatíveis com instâncias expansíveis T3. As instâncias T3 apresentam um bom custo-benefício para usar seu software de licença BYOL elegível em hardware dedicado. O menor espaço de vCPU das instâncias T3 permite consolidar seus workloads em menos hosts e maximizar a utilização da licença por núcleo.

Os hosts dedicados T3 são mais adequados para executar o software BYOL com utilização de CPU baixa a moderada. Isso inclui licenças de software qualificadas por soquete, por núcleo ou por VM, como Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux e Oracle Database. Exemplos de workloads adequadas a hosts dedicados T3 são bancos de dados pequenos e médios, desktops virtuais, ambientes de desenvolvimento e teste, repositórios de código e protótipos de produtos. Os hosts dedicados T3 não são recomendados para workloads com alta utilização sustentada da CPU ou para workloads que experimentem intermitências de CPU correlacionadas simultaneamente.

As instâncias T3 em Hosts Dedicados usam o mesmo modelo de crédito que as instâncias T3 em hardware de locação compartilhada. No entanto, eles são compatíveis apenas com o modo de crédito **standard**; não com o modo de crédito **unlimited**. No modo **standard**, instâncias T3 em Hosts Dedicados ganham, gastam e acumulam créditos da mesma forma que instâncias intermitentes em hardware de locação compartilhada. Elas fornecem performance de CPU de linha de base com capacidade de intermitência acima do nível de linha de base. Para intermitências acima da linha de base, a instância gasta os créditos acumulados no seu saldo de créditos de CPU. Quando os créditos acumulados estão esgotados, a utilização da CPU é reduzida para o nível de linha de base. Para mais informações sobre o modo **standard**, consulte [Como funcionam as instâncias expansíveis padrão \(p. 186\)](#).

Os hosts dedicados T3 oferecem suporte a todos os recursos oferecidos pelos hosts dedicados do Amazon EC2, incluindo vários tamanhos de instância em um único host, grupos de recursos de host e BYOL.

Tamanhos e configurações de instância T3 compatíveis

Os hosts dedicados T3 executam instâncias T3 estáveis de uso geral que compartilham recursos de CPU do host, fornecendo uma performance de CPU de linha de base e a capacidade de intermitência para um nível mais alto quando necessário. Isso permite que os hosts dedicados T3, que têm 48 núcleos, suportem

até no máximo 192 instâncias por host. Para utilizar os recursos do host de forma eficiente e fornecer a melhor performance de instância, o algoritmo de posicionamento de instância do Amazon EC2 calcula automaticamente o número de instâncias suportadas e combinações de tamanho de instância que podem ser iniciadas no host.

Os hosts dedicados T3 oferecem suporte a vários tipos de instância no mesmo host. Todos os tamanhos de instâncias T3 são compatíveis em um Host Dedicado. Você pode executar diferentes combinações de instâncias T3 até o limite de CPU do host.

A tabela a seguir lista os tipos de instância compatíveis, resume a performance de cada tipo de instância e indica o número máximo de instâncias de cada tamanho que pode ser lançado.

Tipo de instância	vCPUs	Memória (GiB)	Utilização da linha de base de CPU por vCPU	Largura de banda em pico de rede (Gbps)	Largura de banda de pico do Amazon EBS (Mbps)	Número máximo de instâncias por Host Dedicado
t3.nano	0,5	5%	5	Até 2.085	192	
t3.micro	1	10%	5	Até 2.085	192	
t3.small	2	20%	5	Até 2.085	192	
t3.medium	4	20%	5	Até 2.085	192	
t3.large	8	30%	5	2.780	96	
t3.xlarge	16	40%	5	2.780	48	
t3.2xlarge	32	40%	5	2.780	24	

Monitorar a utilização da CPU para hosts dedicados T3

Você pode usar a métrica `DedicatedHostCPUUtilization` do Amazon CloudWatch para monitorar a utilização da vCPU de um Host Dedicado. A métrica está disponível no namespace `EC2` e na dimensão `Per-Host-Metrics`. Para obter mais informações, consulte [Métricas de Host Dedicado \(p. 906\)](#).

Restrições do Hosts dedicados

Antes de alocar Hosts dedicados, observe as seguintes limitações e restrições:

- Para executar o RHEL, o SUSE Linux e o SQL Server no Hosts dedicados, você deve trazer suas próprias AMIs. As AMIs do RHEL, SUSE Linux e SQL Server oferecidas pela AWS ou disponíveis no AWS Marketplace não podem ser usadas com os hosts dedicados. Para obter mais informações sobre como criar sua própria AMI, consulte [Traga sua própria licença \(p. 350\)](#).

Essa restrição não se aplica a hosts alocados para instâncias de alta memória (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`). As AMIs do RHEL e do SUSE Linux oferecidas pela AWS ou disponíveis no AWS Marketplace podem ser usadas com esses hosts.

- É possível alocar até dois Hosts dedicados sob demanda por família de instância, por região. É possível solicitar um aumento de limite: [Solicitar aumento de limite de alocação em Hosts dedicados do Amazon EC2](#).
- As instâncias que são executadas em um Host dedicado somente podem ser iniciadas em uma VPC.
- Grupos de Auto Scaling são compatíveis ao usar um modelo de execução que especifica um grupo de recursos de host. Para obter mais informações, consulte [Criar um modelo de execução para um grupo de Auto Scaling](#) no Guia do usuário do Amazon EC2 Auto Scaling.

- Não há suporte para instâncias do Amazon RDS.
- O nível de uso gratuito da AWS não está disponível para hosts dedicados.
- O controle de posicionamento de instância se refere ao gerenciamento de execuções de instâncias em Hosts dedicados. Não é possível iniciar o Hosts dedicados em placement groups.

Definição de preço e faturamento

O preço de um Host dedicado varia de acordo com a opção de pagamento.

Opções de pagamento

- [Hosts dedicados sob demanda \(p. 353\)](#)
- [Dedicated Host Reservations \(p. 353\)](#)
- [Savings Plans \(p. 354\)](#)
- [Definição de preço para o Windows Server no Hosts dedicados \(p. 354\)](#)

Hosts dedicados sob demanda

O faturamento sob demanda é automaticamente ativado quando você aloca um Host dedicado à sua conta.

O preço sob demanda para um Host dedicado varia por família de instância e por região. É cobrado por segundo (com mínimo de 60 segundos) por Host dedicado ativo, independentemente da quantidade ou do tamanho das instâncias que você optar por executar nele. Para obter mais informações sobre a definição de preço sob demanda, consulte [Amazon EC2 Hosts dedicados On-Demand Pricing](#) (Definição de preço sob demanda).

Você pode liberar um Host dedicado sob demanda a qualquer momento para parar de acumular cobranças para ele. Para obter informações sobre como liberar um Host dedicado, consulte [Liberar Hosts dedicados \(p. 369\)](#).

Dedicated Host Reservations

Os Reservas de hosts dedicados fornecem um desconto de faturamento em comparação com a execução de Hosts dedicados sob demanda. Há três opções de pagamento disponíveis para as reservas:

- Sem pagamento adiantado — as reservas sem pagamento adiantado fornecem um desconto no uso do Host dedicado durante um período de vigência e não requerem pagamento adiantado. Disponível para períodos de vigência de um e três anos. Apenas algumas famílias de instâncias oferecem suporte para o período de vigência de três anos para a opção Sem reservas antecipadas.
- Pagamento adiantado parcial — deve ser feito o pagamento adiantado de uma parte da reserva, e as horas restantes do período de vigência são cobradas com uma taxa com desconto. Disponível para períodos de vigência de um e três anos.
- Pagamento integral adiantado — fornece o menor preço. Disponível para períodos de vigência de um e três anos e abrange todo o custo do período antecipadamente, sem nenhuma outra cobrança futura.

Você deve ter Hosts dedicados ativos em sua conta para poder comprar reservas. Cada reserva pode cobrir um ou mais hosts que oferecem suporte para a mesma família de instâncias em uma única zona de disponibilidade. As reservas são aplicadas à família da instância do host e não ao tamanho da instância. Se você tiver três Hosts dedicados com diferentes tamanhos de instâncias (`m4.xlarge`, `m4.medium` e `m4.large`), poderá associar uma única reserva `m4` a todos esses Hosts dedicados. A família de instâncias e a zona de disponibilidade da reserva devem corresponder aos hosts dedicados aos quais você quer se associar.

Quando uma reserva for associada a um Host dedicado, o Host dedicado não poderá ser liberado até que o prazo da reserva termine.

Para obter mais informações sobre a definição de preço de reservas, consulte [Definição de preço de Hosts dedicados do Amazon EC2](#).

Savings Plans

Savings Plans são um modelo de definição de preço flexível que oferece economias significativas em Instâncias on-demand. Com o Savings Plans, você se compromete com uma quantidade consistente de uso, em USD por hora, por um período de vigência de um ou de três anos. Isso oferece a flexibilidade de usar Hosts dedicados que melhor atendam às suas necessidades e continuar economizando dinheiro, em vez de se comprometer com um Host dedicado específico. Para obter mais informações, consulte o [Guia do usuário do AWS Savings Plans](#).

Definição de preço para o Windows Server no Hosts dedicados

Conforme os termos de licenciamento da Microsoft, você pode trazer suas licenças de Windows Server e SQL Server para o Hosts dedicados. Não há cobrança adicional para uso de software caso você opte por trazer as próprias licenças.

Além disso, você também pode usar as AMIs do Windows Server fornecidas pela Amazon para executar as versões mais recentes do Windows Server no Hosts dedicados. Isso é comum para cenários nos quais você tem licenças do SQL Server qualificadas para execução no Hosts dedicados, mas precisa do Windows Server para executar a workload do SQL Server. As AMIs do Windows Server fornecidas pela Amazon são compatíveis somente com os [tipos de instância da geração atual \(p. 149\)](#). Para obter mais informações, consulte [Amazon EC2 Dedicated Hosts Pricing \(Definição de preço de hosts dedicados do Amazon EC2\)](#).

Como trabalhar com o Hosts dedicados

Para usar um Host dedicado, primeiro aloque os hosts a serem usados na sua conta. Depois, execute instâncias nos hosts especificando a locação do host da instância. Você deve selecionar um host específico no qual executar a instância ou permitir que ela seja executada em qualquer host que tenha o posicionamento automático habilitado e corresponda ao seu tipo de instância. Quando uma instância é interrompida e reiniciada, a configuração Afinidade de host determina se ela será reiniciada no mesmo host ou em um host diferente.

Se você não precisar mais de um host sob demanda, poderá interromper as instâncias em execução no host, direcioná-las para execução em um host diferente e liberar o host.

Hosts dedicados também estão integrados ao AWS License Manager. Com o License Manager, é possível criar um grupo de recursos de host, que é uma coleção de Hosts dedicados gerenciados como uma única entidade. Ao criar um grupo de recursos de host, especifique as preferências de gerenciamento de host, como alocação automática e liberação automática, para os Hosts dedicados. Isso permite que você execute instâncias em Hosts dedicados sem alocar e gerenciar manualmente esses hosts. Para obter mais informações, consulte [Grupos de recursos de host](#) no Guia do usuário do AWS License Manager.

Tópicos

- [Alocar Hosts dedicados \(p. 355\)](#)
- [Execute instâncias em um Host dedicado. \(p. 357\)](#)
- [Execute instâncias em um grupo de recursos de host. \(p. 359\)](#)
- [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#)
- [Modificar posicionamento automático de Host dedicado \(p. 361\)](#)
- [Modificar os tipos de instância compatíveis \(p. 362\)](#)
- [Modificar locação e da afinidade de instâncias \(p. 364\)](#)
- [Visualização do Hosts dedicados \(p. 365\)](#)

- [Marcação de Hosts dedicados \(p. 367\)](#)
- [Monitorar Hosts dedicados \(p. 368\)](#)
- [Liberar Hosts dedicados \(p. 369\)](#)
- [Comprar Reservas de hosts dedicados \(p. 370\)](#)
- [Visualizar reservas de Host dedicado \(p. 372\)](#)
- [Atribuir tag de Reservas de hosts dedicados \(p. 372\)](#)

Alocar Hosts dedicados

Para começar a usar o Hosts dedicados, você deve alocar o Hosts dedicados à sua conta usando o console do Amazon EC2 ou as ferramentas de linha de comando. Depois da alocação do Host dedicado, a capacidade do Host dedicado é imediatamente disponibilizada em sua conta, e você pode começar a executar instâncias no Host dedicado.

O suporte para vários tamanhos de instância da mesma família de instâncias no mesmo Host Dedicado está disponível para as seguintes famílias de instâncias: c5, m5, r5, c5n, r5n e m5n. Outras famílias de instâncias suportam apenas um tamanho de instância no mesmo Host dedicado.

Devido a uma limitação de hardware com o Hosts dedicados tipo N, como C5n, M5n e R5n, você não pode misturar tamanhos de instância menores (`large`, `xlarge`, `2xlarge`) com tamanhos de instância maiores (`4xlarge`, `9xlarge`, `18xlarge` e `.metal`). Se você precisar de tamanhos de instância menores e maiores em hosts do tipo N ao mesmo tempo, será necessário alocar hosts separados para os tamanhos de instância menores e maiores.

É possível alocar um Host dedicado usando os métodos a seguir.

New console

Como alocar um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Hosts dedicados e Allocate Host dedicado (Alocar Host dedicado).
3. Em Instance family (Família de instâncias), escolha a família de instâncias do Host dedicado.
4. Especifique se o Host dedicado oferece suporte a vários tipos de instância na família de instâncias selecionada ou a um único tipo específico de instância. Faça uma das coisas a seguir.
 - Para configurar o Host dedicado para oferecer suporte a vários tipos de instância na família de instâncias selecionada, em Support multiple instance types (Oferecer suporte a vários tipos de instância), escolha Enable (Habilitar). Isso permitirá executar diferentes tipos de instância da família de instâncias selecionada no Host dedicado. Por exemplo, se você escolher a família de instâncias m5 e escolher essa opção, poderá executar instâncias `m5.xlarge` e `m5.4xlarge` no Host dedicado.
 - Para configurar o Host dedicado a fim de oferecer suporte a um tipo de instância na família de instâncias selecionada, desmarque Support multiple instance types (Oferecer suporte a vários tipos de instância) e, em Instance type (Tipo de instância), escolha o tipo de instância ao qual oferecer suporte. Isso permite que você execute um único tipo de instância no Host dedicado. Por exemplo, se você escolher essa opção e especificar `m5.4xlarge` como o tipo de instância compatível, poderá executar apenas instâncias `m5.4xlarge` no Host dedicado.
5. Em Availability Zone (Zona de disponibilidade), escolha a zona de disponibilidade na qual o Host dedicado será alocado.
6. Para permitir que o Host dedicado aceite lançamentos de instância não direcionada compatíveis com o tipo de instância, para Instance auto-placement (Autoposicionamento da instância), selecione Enable (Habilitar). Para obter mais informações sobre posicionamento automático, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).

7. Para habilitar a recuperação do host para o Host dedicado, em Host recovery (Recuperação do host), selecione Enable (Habilitar). Para obter mais informações, consulte [Recuperação do host \(p. 378\)](#).
8. Em Quantity (Quantidade), insira o número de Hosts dedicados a ser alocado.
9. (Opcional) Escolha Add new tag (Adicionar nova tag) e digite uma chave de tag e um valor de tag.
10. Escolha Allocate.

Old console

Como alocar um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados, Allocate Host dedicado (Alocar dh).
3. Em Instance family (Família de instâncias), escolha a família de instâncias do Host dedicado.
4. Especifique se o Host dedicado oferece suporte a vários tipos de instância na família de instâncias selecionada ou a um único tipo específico de instância. Faça uma das coisas a seguir.
 - Para configurar o Host dedicado para oferecer suporte a vários tipos de instância na família de instâncias selecionada, selecione Support multiple instance types (Oferecer suporte a vários tipos de instância). Isso permitirá executar diferentes tipos de instância da família de instâncias selecionada no Host dedicado. Por exemplo, se você escolher a família de instâncias m5 e escolher essa opção, poderá executar instâncias m5.xlarge e m5.4xlarge no Host dedicado. A família de instâncias deve ser capacitada pelo sistema Nitro.
 - Para configurar o Host dedicado a fim de oferecer suporte a um tipo de instância na família de instâncias selecionada, desmarque Support multiple instance types (Oferecer suporte a vários tipos de instância) e, em Instance type (Tipo de instância), escolha o tipo de instância ao qual oferecer suporte. Isso permite que você execute um único tipo de instância no Host dedicado. Por exemplo, se você escolher essa opção e especificar m5.4xlarge como o tipo de instância compatível, poderá executar apenas instâncias m5.4xlarge no Host dedicado.
5. Em Availability Zone (Zona de disponibilidade), escolha a zona de disponibilidade na qual o Host dedicado será alocado.
6. Para permitir que o Host dedicado aceite lançamentos de instância não direcionada compatíveis com o tipo de instância, para Instance auto-placement (Autoposicionamento da instância), selecione Enable (Habilitar). Para obter mais informações sobre posicionamento automático, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).
7. Para habilitar a recuperação do host para o Host dedicado, para Host recovery (Recuperação do host), selecione Enable (Habilitar). Para obter mais informações, consulte [Recuperação do host \(p. 378\)](#).
8. Em Quantity (Quantidade), insira o número de Hosts dedicados a ser alocado.
9. (Opcional) Escolha Add Tag (Adicionar tag) e digite uma chave de tag e um valor de tag.
10. Escolha Allocate host (Alocar host).

AWS CLI

Como alocar um Host dedicado

Use o comando `allocate-hosts` da AWS CLI. O comando a seguir aloca um Host dedicado que oferece suporte a vários tipos de instância da família de instâncias m5 na zona de disponibilidade us-east-1a. O host também tem a recuperação do host habilitada e o posicionamento automático desabilitado.

```
aws ec2 allocate-hosts --instance-family "m5" --availability-zone "us-east-1a" --auto-placement "off" --host-recovery "on" --quantity 1
```

O comando a seguir aloca um Host dedicado que oferece suporte a execuções de instâncias m4.large não direcionadas na zona de disponibilidade eu-west-1a, habilita recuperação do host e aplica uma tag com uma chave de purpose e um valor de production.

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a"  
--auto-placement "on" --host-recovery "on" --quantity 1 --tag-specifications  
'ResourceType=dedicated-host',Tags=[{Key=purpose,Value=production}]'
```

PowerShell

Como alocar um Host dedicado

Use o comando [New-EC2Host](#) do AWS Tools for Windows PowerShell. O comando a seguir aloca um Host dedicado que oferece suporte a vários tipos de instância da família de instâncias m5 na zona de disponibilidade us-east-1a. O host também tem a recuperação do host habilitada e o posicionamento automático desabilitado.

```
PS C:\> New-EC2Host -InstanceFamily m5 -AvailabilityZone us-east-1a -AutoPlacement Off  
-HostRecovery On -Quantity 1
```

Os comandos a seguir alocam um Host dedicado que oferece suporte a execuções de instâncias m4.large não destinadas na zona de disponibilidade eu-west-1a, habilitam recuperação do host e aplicam uma tag com uma chave de purpose e um valor de production.

O parâmetro TagSpecification usado para marcar um Host dedicado na criação requer um objeto que especifique o tipo de recurso a ser marcado, a chave e o valor da tag. Os comandos a seguir criam o objeto necessário.

```
PS C:\> $tag = @{ Key="purpose"; Value="production" }  
PS C:\> $tagspec = new-object Amazon.EC2.Model.TagSpecification  
PS C:\> $tagspec.ResourceType = "dedicated-host"  
PS C:\> $tagspec.Tags.Add($tag)
```

O comando a seguir aloca o Host dedicado e aplica a tag especificada no objeto \$tagspec.

```
PS C:\> New-EC2Host -InstanceType m4.large -AvailabilityZone eu-west-1a -  
AutoPlacement On -HostRecovery On -Quantity 1 -TagSpecification $tagspec
```

Execute instâncias em um Host dedicado.

Depois de alocar um Host dedicado, você pode executar instâncias nele. Você não pode executar instâncias com locação de host se não tiver Hosts dedicados ativos com capacidade suficiente disponível para o tipo de instância que está executando.

Note

As instâncias executadas em Hosts dedicados somente podem ser iniciadas em uma VPC. Para obter mais informações, consulte [Introdução à VPC](#).

Antes de executar as instâncias, observe as limitações. Para obter mais informações, consulte [Restrições do Hosts dedicados \(p. 352\)](#).

É possível executar uma instância em um Host dedicado usando os métodos a seguir.

Console

Para executar uma instância em um Host dedicado específico na página de Hosts dedicados

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. Escolha Hosts dedicados no painel de navegação.
3. Na página Hosts dedicados, selecione um host e escolha Actions (Ações), Launch Instance(s) onto Host (Executar instâncias no host).
4. Selecione uma AMI na lista. AMIs do SQL Server, do SUSE e do RHEL fornecidas pelo Amazon EC2 não podem ser usadas com Hosts dedicados.
5. Na página Choose an Instance Type (Escolher um tipo de instância), selecione o tipo de instância a ser executada e escolha Next: Configure Instance Details (Próximo: configurar detalhes da instância).

Se o Host dedicado oferecer suporte a um único tipo de instância, o tipo de instância com suporte será selecionado por padrão e não poderá ser alterado.

Se o Host dedicado oferecer suporte a vários tipos de instância, será necessário selecionar um tipo de instância na família de instâncias com suporte de acordo com a capacidade de instância disponível do Host dedicado. Recomendamos que você execute primeiro os tamanhos de instância maiores e preencha a capacidade restante da instância com os tamanhos de instância menores, conforme necessário.

6. Na página Configure Instance Details (Configurar detalhes da instância), defina as configurações de instância para atender às suas necessidades. Em Affinity (Afinidade), escolha uma das seguintes opções:
 - Off (Desativado) — a instância é executada no host especificado, mas não é garantido que será reiniciada no mesmo Host dedicado se for interrompida.
 - Host — se for interrompida, a instância sempre será reiniciada nesse host específico.

Para obter mais informações sobre afinidade, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).

As opções Tenancy (Locação) e Host são pré-configuradas com base no host selecionado.

7. Escolha Review and Launch.
8. Na página Review Instance Launch, escolha Launch.
9. Quando solicitado, selecione um par de chaves existente ou crie um novo e, em seguida, selecione Launch Instances (Executar instâncias).

Para executar uma instância em um Host dedicado usando o assistente de execução de instâncias

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias), Launch Instance (Executar instância).
3. Selecione uma AMI na lista. AMIs do SQL Server, do SUSE e do RHEL fornecidas pelo Amazon EC2 não podem ser usadas com Hosts dedicados.
4. Selecione o tipo de instância a ser executada e escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), defina as configurações de instância para atender às suas necessidades e defina as seguintes configurações, que são específicas de um Host dedicado:
 - Locação — escolha Host dedicado - Launch this instance on a Host dedicated (dh – Executar esta instância em um dh).
 - Host — escolha Use auto-placement (Usar posicionamento automático) para executar a instância em qualquer Host dedicado que tenha o posicionamento automático habilitado ou selecione um Host dedicado específico na lista. A lista exibe apenas Hosts dedicados que oferecem suporte ao tipo de instância selecionado.

- Afinidade — escolha uma das seguintes opções:
 - Off (Desativado) — a instância é executada no host especificado, mas não é garantido que será reiniciada nele se for interrompida.
 - Host — se for interrompida, a instância sempre será reiniciada no host especificado.

Para obter mais informações, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).

Se você não estiver vendo essas configurações, verifique se selecionou uma VPC no menu Network (Rede).

6. Escolha Review and Launch.
7. Na página Review Instance Launch, escolha Launch.
8. Quando solicitado, selecione um par de chaves existente ou crie um novo e, em seguida, selecione Launch Instances (Executar instâncias).

AWS CLI

Como iniciar uma instância em um Host dedicado

Use o comando `run-instances` da AWS CLI e especifique a afinidade da instância, a locação e o host no parâmetro de solicitação `Placement`.

PowerShell

Como iniciar uma instância em um Host dedicado

Use o comando `New-EC2Instance` do AWS Tools for Windows PowerShell e especifique a afinidade da instância, a locação e o host no parâmetro de solicitação `Placement`.

Execute instâncias em um grupo de recursos de host.

Quando você executa uma instância em um grupo de recursos de host que tem um Host dedicado com capacidade de instância disponível, o Amazon EC2 executa a instância nesse host. Se o grupo de recursos de host não tiver um host com capacidade de instância disponível, o Amazon EC2 aloca automaticamente um novo host no grupo de recursos de host e, depois, executará a instância nesse host. Para obter mais informações, consulte [Grupos de recursos de host](#) no Guia do usuário do AWS License Manager.

Requisitos e limites

- Você deve associar uma configuração de licença baseada em núcleo ou soquete à AMI.
- Não é possível usar as AMIs do SQL Server, do SUSE ou do RHEL fornecidas pelo Amazon EC2 com os Hosts dedicados.
- Você não pode segmentar um host específico escolhendo um ID de host e não é possível habilitar a afinidade de instâncias ao executar uma instância em um grupo de recursos de host.

É possível executar uma instância em um grupo de recursos de host usando os métodos a seguir.

New console

Como executar uma instância em um grupo de recursos de host

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias), Launch Instances (Executar instâncias).
3. Selecione uma AMI.

4. Selecione o tipo de instância a ser executada e escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), defina as configurações de instância para atender às suas necessidades e faça o seguinte:
 - a. Para Tenancy (Locação), escolha Host dedicado.
 - b. Para Host resource group (Grupo de recursos de host), escolha Launch instance into a host resource group (Executar instância em um grupo de recursos de host).
 - c. Para Host resource group name (Nome do grupo de recursos de host), escolha o grupo de recursos de host no qual a instância será executada.
6. Escolha Review and Launch.
7. Na página Review Instance Launch, escolha Launch.
8. Quando solicitado, selecione um par de chaves existente ou crie um novo e, em seguida, selecione Launch Instances (Executar instâncias).

Old console

Como executar uma instância em um grupo de recursos de host

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias), Launch Instance (Executar instância).
3. Selecione uma AMI.
4. Selecione o tipo de instância a ser executada e escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), defina as configurações de instância para atender às suas necessidades e faça o seguinte:
 - a. Para Tenancy (Locação), escolha Host dedicado.
 - b. Para Host resource group (Grupo de recursos de host), escolha Launch instance into a host resource group (Executar instância em um grupo de recursos de host).
 - c. Para Host resource group name (Nome do grupo de recursos de host), escolha o grupo de recursos de host no qual a instância será executada.
6. Escolha Review and Launch.
7. Na página Review Instance Launch, escolha Launch.
8. Quando solicitado, selecione um par de chaves existente ou crie um novo e, em seguida, selecione Launch Instances (Executar instâncias).

AWS CLI

Como executar uma instância em um grupo de recursos de host

Use o comando `run-instances` da AWS CLI e, no parâmetro de solicitação `Placement`, omita a opção `Tenancy` e especifique o ARN do grupo de recursos do host.

PowerShell

Como executar uma instância em um grupo de recursos de host

Use o comando `New-EC2Instance` do AWS Tools for Windows PowerShell e, no parâmetro de solicitação `Placement`, omita a opção `Tenancy` e especifique o ARN do grupo de recursos do host.

Noções básicas sobre posicionamento automático e afinidade

O controle de posicionamento do Hosts dedicados ocorre em nível de instância e de host.

Posicionamento automático

O posicionamento automático é configurado no nível do host. Ele permite que você gerencie se as instâncias são executadas em um host específico ou em qualquer host disponível com as configurações correspondentes.

Quando o posicionamento automático de um Host dedicado está desabilitado, ele só aceita execuções de instâncias de locação Host que especificam seu ID exclusivo de host. Trata-se da configuração padrão para novos Hosts dedicados.

Quando o posicionamento automático de um Host dedicado está habilitado, ele aceita todas as execuções de instâncias não direcionadas que correspondam à configuração do tipo de instância.

Ao executar uma instância, você precisa configurar sua locação. A execução de uma instância em um Host dedicado sem fornecer um `HostId` específico permite que você a execute em qualquer Host dedicado que tenha o posicionamento automático habilitado e corresponda ao seu tipo de instância.

Afinidade de host

A afinidade de host é configurada no nível da instância. Ela estabelece uma relação de execução entre uma instância e um Host dedicado.

Quando a afinidade é definida como `Host`, uma instância executada em um host específico sempre é reiniciada no mesmo host se for interrompida. Isso se aplica a execuções direcionadas e não direcionadas.

Quando a afinidade estiver definida como `Off` e você parar e reiniciar a instância, ela poderá ser reiniciada em qualquer host disponível. Contudo, ela tenta ser executada novamente no último Host dedicado em que estava em execução (com base no melhor esforço).

Modificar posicionamento automático de Host dedicado

É possível modificar as configurações de posicionamento automático de um Host dedicado depois de alocá-lo à sua conta da AWS, usando um dos métodos a seguir.

New console

Como modificar o posicionamento automático de um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione um host e escolha Actions (Ações), Modify host (Modificar host).
4. Em Instance auto-placement (Posicionamento automático da instância), escolha Enable (Habilitar) para habilitar o posicionamento automático ou desmarque Enable (Habilitar) para desabilitar o posicionamento automático. Para obter mais informações, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).
5. Escolha Save (Salvar).

Old console

Como modificar o posicionamento automático de um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Hosts dedicados no painel de navegação.
3. Na página Hosts dedicados, selecione um host e escolha Actions (Ações) e, em seguida, escolha Modify Auto-Placement (Modificar posicionamento automático).
4. Na janela Modify Auto-Placement (Modificar posicionamento automático), em Allow instance auto-placement (Permitir posicionamento automático de instâncias), escolha Yes (Sim) para habilitar o

posicionamento automático ou escolha No (Não) para desabilitar o posicionamento automático. Para obter mais informações, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).

5. Escolha Save (Salvar).

AWS CLI

Como modificar o posicionamento automático de um Host dedicado

Use o comando [modify-hosts](#) da AWS CLI. O exemplo a seguir habilita o posicionamento automático para o Host dedicado especificado.

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

PowerShell

Como modificar o posicionamento automático de um Host dedicado

Use o comando [Edit-EC2Host](#) do AWS Tools for Windows PowerShell. O exemplo a seguir habilita o posicionamento automático para o Host dedicado especificado.

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

Modificar os tipos de instância compatíveis

A compatibilidade com vários tipos de instância no mesmo host dedicado está disponível para as seguintes famílias de instâncias: c5, m5, r5, c5n, r5n e m5n. Outras famílias de instâncias oferecem suporte apenas a um único tipo de instância no mesmo Host dedicado.

É possível alocar um Host dedicado usando os métodos a seguir.

É possível modificar um Host dedicado para alterar os tipos de instância aos quais ele oferece suporte. Se ele oferecer suporte a um único tipo de instância no momento, você poderá modificá-lo para oferecer suporte a vários tipos de instância dentro dessa família de instâncias. De forma semelhante, se ele oferecer suporte a vários tipos de instância, você poderá modificá-lo para oferecer suporte somente a um tipo específico de instância.

Para modificar o Host dedicado para oferecer suporte a vários tipos de instância, primeiro interrompa todas as instâncias em execução no host. Essa modificação leva aproximadamente 10 minutos para ser concluída. O Host dedicado faz a transição para o estado pending enquanto as modificações estão em andamento. Não é possível iniciar instâncias interrompidas ou executar novas instâncias no Host dedicado enquanto ele estiver no estado pending.

Para modificar um Host dedicado compatível com vários tipos de instância para que ofereça suporte a um tipo específico de instância, o host não deve ter nenhuma instância em execução, ou as instâncias em execução devem ser do tipo ao qual você deseja que o host ofereça suporte. Por exemplo, para modificar um host que oferece suporte a vários tipos de instância na família de instâncias m5 para oferecer suporte apenas a instâncias m5 . large, o Host dedicado não deve ter nenhuma instância em execução ou ter apenas instâncias m5 . large em execução.

É possível modificar os tipos de instância compatíveis usando um dos métodos a seguir.

New console

Como modificar os tipos de instância compatíveis de um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha Host Dedicado.
3. Selecione o Host dedicado a ser modificado e escolha Actions (Ações), Modify host (Modificar host).
4. Dependendo da configuração atual do Host dedicado, siga um destes procedimentos:
 - Atualmente, se o Host dedicado oferecer suporte a um tipo de instância específico, o Support multiple instance types (Oferecer suporte a vários tipos de instância) não será habilitado e o Instance type (Tipo de instância) listará o tipo de instância compatível. Para modificar o host para oferecer suporte a vários tipos na família de instâncias atual, em Support multiple instance types (Oferecer suporte a vários tipos de instância), escolha Enable (Habilitar).

Primeiro você deve interromper todas as instâncias em execução no host antes de modificá-lo para oferecer suporte a vários tipos de instância.

- Atualmente, se o Host dedicado oferecer suporte a vários tipos de instância em uma família de instâncias, Enabled (Habilitado) estará selecionado em Support multiple instance types (Oferecer suporte a vários tipos de instância). Para modificar o host para oferecer suporte a um tipo específico de instância, em Support multiple instance types (Oferecer suporte a vários tipos de instância), desmarque Enable (Habilitar) e, em Instance type (Tipo de instância), selecione o tipo de instância específico ao qual oferecer suporte.

Não é possível alterar a família de instâncias compatível do Host dedicado.

5. Escolha Save (Salvar).

Old console

Como modificar os tipos de instância compatíveis de um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Host Dedicado.
3. Selecione o Host dedicado a ser modificado e escolha Actions (Ações), Modify Supported Instance Types (Modificar os tipos de instância compatíveis).
4. Dependendo da configuração atual do Host dedicado, siga um destes procedimentos:
 - Se atualmente o Host dedicado oferecer suporte a um tipo específico de instância, No (Não) estará selecionado para Support multiple instance types (Oferecer suporte a vários tipos de instância). Para modificar o host para oferecer suporte a vários tipos na família de instâncias atual, em Support multiple instance types (Oferecer suporte a vários tipos de instância) selecione Yes (Sim).

Primeiro você deve interromper todas as instâncias em execução no host antes de modificá-lo para oferecer suporte a vários tipos de instância.

- Se, atualmente, o Host dedicado oferecer suporte a vários tipos de instância em uma família de instâncias, Yes (Sim) estará selecionado para Support multiple instance types (Oferecer suporte a vários tipos de instância), e Instance family (Família de instâncias) exibirá a família de instâncias compatível. Para modificar o host para oferecer suporte a um tipo específico de instância, em Support multiple instance types (Oferecer suporte a vários tipos de instância), selecione No (Não) e, para Instance type (Tipo de instância), selecione o tipo de instância específico ao qual oferecer suporte.

Não é possível alterar a família de instâncias compatível do Host dedicado.

5. Escolha Save (Salvar).

AWS CLI

Como modificar os tipos de instância compatíveis de um Host dedicado

Use o comando [modify-hosts](#) da AWS CLI.

O comando a seguir modifica um Host dedicado para oferecer suporte a vários tipos de instância na família de instâncias m5.

```
aws ec2 modify-hosts --instance-family m5 --host-ids h-012a3456b7890cdef
```

O comando a seguir modifica um Host dedicado para oferecer suporte apenas a instâncias m5.xlarge.

```
aws ec2 modify-hosts --instance-type m5.xlarge --instance-family --host-ids h-012a3456b7890cdef
```

PowerShell

Como modificar os tipos de instância compatíveis de um Host dedicado

Use o comando [Edit-EC2Host](#) do AWS Tools for Windows PowerShell.

O comando a seguir modifica um Host dedicado para oferecer suporte a vários tipos de instância na família de instâncias m5.

```
PS C:\> Edit-EC2Host --InstanceFamily m5 --HostId h-012a3456b7890cdef
```

O comando a seguir modifica um Host dedicado para oferecer suporte apenas a instâncias m5.xlarge.

```
PS C:\> Edit-EC2Host --InstanceType m5.xlarge --HostId h-012a3456b7890cdef
```

Modificar locação e da afinidade de instâncias

Você pode alterar a locação de uma instância de dedicated para host, ou de host para dedicated, depois de executá-la. Também é possível modificar a afinidade entre a instância e o host. Para modificar a locação ou a afinidade da instância, a instância deve estar no estado stopped.

Note

Para instâncias T3, você não pode alterar a locação de dedicated para host, ou de host para dedicated. A tentativa de fazer uma dessas alterações de locação não compatíveis resulta no código de erro InvalidTenancy.

É possível modificar a locação e a afinidade de uma instância usando os métodos a seguir.

Console

Como modificar a locação ou a afinidade da instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Instances (Instâncias) e selecione a instância a ser modificada.
3. Escolha Instance state (Estado da instância), Stop (Interromper).
4. Abra o menu de contexto (clique com o botão direito do mouse) na instância e escolha Instance Settings (Configurações da instância), Modify Instance Placement (Modificar posicionamento da instância).
5. Na página Modify Instance Placement (Modificar posicionamento da instância), configure o seguinte:

- Tenancy (Locação) — escolha um dos seguintes:
 - Run a dedicated hardware instance (Executar uma instância de hardware dedicada) — executa a instância como um Instâncias dedicadas. Para obter mais informações, consulte [Dedicated Instances \(p. 383\)](#).
 - Launch the instance on a Host dedicado (Executar a instância em um dh) — executa a instância em um Host dedicado com afinidade configurável.
- Affinity (Afinidade) — escolha uma das seguintes opções:
 - This instance can run on any one of my hosts (Esta instância pode ser executada em qualquer um dos meus hosts) — A instância é executada em qualquer Host dedicado disponível em uma conta que ofereça suporte ao seu tipo de instância.
 - This instance can only run on the selected host (Esta instância só pode ser executada no host selecionado) — A instância só pode ser executada no Host dedicado selecionado em Target Host (Host de destino).
- Target Host (Host de destino) — selecione o Host dedicado no qual executar a instância. Se nenhum host de destino estiver listado, talvez não haja Hosts dedicados disponíveis e compatíveis em sua conta.

Para obter mais informações, consulte [Noções básicas sobre posicionamento automático e afinidade \(p. 360\)](#).

6. Escolha Save (Salvar).

AWS CLI

Como modificar a locação ou a afinidade da instância

Use o comando [modify-instance-placement](#) da AWS CLI. O exemplo a seguir altera a afinidade da instância especificada de default para host e especifica o Host dedicado com o qual a instância tem afinidade.

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host --  
host-id h-012a3456b7890cdef
```

PowerShell

Como modificar a locação ou a afinidade da instância

Use o comando [Edit-EC2InstancePlacement](#) do AWS Tools for Windows PowerShell. O exemplo a seguir altera a afinidade da instância especificada de default para host e especifica o Host dedicado com o qual a instância tem afinidade.

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -  
HostId h-012a3456b7890cdef
```

Visualização do Hosts dedicados

É possível visualizar os detalhes de um Host dedicado e das Instâncias individuais existentes nele usando os métodos a seguir.

New console

Como exibir os detalhes de um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, selecione Hosts dedicados.
3. Na página Hosts dedicados, selecione um host.
4. Para obter informações sobre o host, escolha Details (Detalhes).

Available vCPUs (vCPUs disponíveis) indica que vCPUs estão disponíveis no Host dedicado para execução de novas instâncias. Por exemplo, um Host dedicado que oferece suporte a vários tipos de instância na família de instâncias c5 e que não tem nenhuma instância em execução nele, tem 72 vCPUs disponíveis. Isso significa que você pode executar diferentes combinações de tipos de instância no Host dedicado para consumir as 72 vCPUs disponíveis.

Para obter informações sobre as instâncias em execução no host, escolha Running instances (Instâncias em execução).

Old console

Como exibir os detalhes de um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Na página Hosts dedicados, selecione um host.
4. Para obter informações sobre o host, escolha Description (Descrição). Available vCPUs (vCPUs disponíveis) indica que vCPUs estão disponíveis no Host dedicado para execução de novas instâncias. Por exemplo, um Host dedicado que oferece suporte a vários tipos de instância na família de instâncias c5 e que não tem nenhuma instância em execução nele, tem 72 vCPUs disponíveis. Isso significa que você pode executar diferentes combinações de tipos de instância no Host dedicado para consumir as 72 vCPUs disponíveis.

Para obter informações sobre as instâncias em execução no host, escolha Instances (Instâncias).

AWS CLI

Como exibir a capacidade de um Host dedicado

Use o comando [describe-hosts](#) da AWS CLI.

O exemplo a seguir usa o comando [describe-hosts](#) (AWS CLI) para visualizar a capacidade de instâncias disponível para um Host dedicado que oferece suporte a vários tipos de instância na família de instâncias c5. O Host dedicado já tem duas instâncias c5.4xlarge e quatro instâncias c5.2xlarge em execução nele.

```
C:\> aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

```
"AvailableInstanceCapacity": [  
    { "AvailableCapacity": 2,  
      "InstanceType": "c5.xlarge",  
      "TotalCapacity": 18 },  
    { "AvailableCapacity": 4,  
      "InstanceType": "c5.large",  
      "TotalCapacity": 36 }  
,  
    "AvailableVCpus": 8
```

PowerShell

Como exibir a capacidade da instância de um Host dedicado

Use o comando [Get-EC2Host](#) do AWS Tools for Windows PowerShell.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

Marcação de Hosts dedicados

Você pode atribuir tags personalizadas aos Host dedicados existentes para categorizá-los de diferentes formas; por exemplo, por objetivo, proprietário ou ambiente. Isso ajuda a localizar rapidamente um host dedicado específico com base na tags personalizadas que você atribuiu. As tags de host dedicado também podem ser usadas para rastreamento de alocação de custos.

Você também pode aplicar tags aos Hosts dedicados no momento da criação. Para obter mais informações, consulte [Alocar Hosts dedicados \(p. 355\)](#).

É possível marcar um Host dedicado usando os métodos a seguir.

New console

Como marcar um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado a ser marcado e escolha Actions (Ações), Manage tags (Gerenciar tags).
4. Na tela Manage tags (Gerenciar tags), escolha Add tag (Adicionar tag) e especifique a chave e o valor da tag.
5. (Opcional) Escolha Add tag (Adicionar tag) para adicionar outras tags ao Host dedicado.
6. Selecione Save changes (Salvar alterações).

Old console

Como marcar um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado a ser marcado e escolha Tags.
4. Escolha Add/Edit Tags.
5. Na caixa de diálogo Add/Edit Tags, selecione Create Tag e, em seguida, especifique a chave e o valor da tag.
6. (Opcional) Escolha Create Tag (Criar tag) para adicionar tags ao Host dedicado.
7. Escolha Save (Salvar).

AWS CLI

Como marcar um Host dedicado

Use o comando da AWS CLI [create-tags](#).

O comando a seguir marca o Host dedicado especificado com Owner=TeamA.

```
aws ec2 create-tags --resources h-abc12345678909876 --tags Key=Owner,Value=TeamA
```

PowerShell

Como marcar um Host dedicado

Use o comando do AWS Tools for Windows PowerShell `New-EC2Tag`.

O comando `New-EC2Tag` precisa de um objeto `Tag`, que especifica o par de chave e valor a ser usado na tag do Host dedicado. Os seguintes comandos criam um objeto `Tag` denominado `$tag` com um par de chave e valor de `Owner` e `TeamA`, respectivamente:

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

O comando a seguir marca o Host dedicado especificado com o objeto `$tag`:

```
PS C:\> New-EC2Tag -Resource h-abc12345678909876 -Tag $tag
```

Monitorar Hosts dedicados

O Amazon EC2 monitora constantemente o estado do seu Hosts dedicados. As atualizações são comunicadas no console do Amazon EC2. É possível exibir informações sobre um Host dedicado usando os métodos a seguir.

Console

Como exibir o estado de um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Localize o Host dedicado na lista e revise o valor na coluna State (Estado).

AWS CLI

Como exibir o estado de um Host dedicado

Use o comando `describe-hosts` da AWS CLI e revise a propriedade `state` no elemento de resposta `hostSet`.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

Como exibir o estado de um Host dedicado

Use o comando `Get-EC2Host` do AWS Tools for Windows PowerShell e revise a propriedade `state` no elemento de resposta `hostSet`.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

A tabela a seguir explica os possíveis estados de um Host dedicado.

Estado	Descrição
available	A AWS não detectou nenhum problema com o Host dedicado. Não estão programados manutenções ou reparos. As instâncias podem ser executadas neste host dedicado.

Estado	Descrição
<code>released</code>	O Host dedicado foi liberado. O ID do host não está mais uso. Os hosts liberados não podem ser reutilizados.
<code>under-assessment</code>	A AWS está explorando um possível problema com o host dedicado. Se for necessário executar uma ação, você será notificado pelo AWS Management Console ou por e-mail. As instâncias não podem ser executadas em um Host dedicado neste estado.
<code>pending</code>	O Host dedicado não pode ser usado para execução de novas instâncias. Ele está sendo modificado para oferecer suporte a vários tipos de instância (p. 362) , ou uma recuperação de host (p. 378) está em andamento.
<code>permanent-failure</code>	Uma falha irrecuperável foi detectada. Você receberá um aviso de remoção por meio de suas instâncias e por e-mail. Suas instâncias podem continuar a ser executadas. Se você interromper ou encerrar todas as instâncias de um host dedicado neste estado, a AWS desativará o host. A AWS não reinicia instâncias nesse estado. As instâncias não podem ser executadas no Hosts dedicados neste estado.
<code>released-permanent-failure</code>	A AWS libera permanentemente hosts dedicados que falharam e não têm mais instâncias em execução. O ID do Host dedicado não está mais disponível para uso.

Liberar Hosts dedicados

Todas as instâncias em execução no Host dedicado devem ser interrompidas para que você possa liberar o host. Essas instâncias podem ser migradas para outros Hosts dedicados de sua conta para que você possa continuar as usando. Estas etapas se aplicam somente a Hosts dedicados sob demanda.

É possível liberar um Host dedicado usando os métodos a seguir.

New console

Como liberar um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Na página Hosts dedicados, selecione o Host dedicado a ser liberado.
4. Escolha Actions (Ações), Release host (Liberar host).
5. Para confirmar, escolha Release (Liberar).

Old console

Como liberar um Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Hosts dedicados no painel de navegação.
3. Na página Hosts dedicados, selecione o Host dedicado a ser liberado.
4. Escolha Actions (Ações), Release Hosts (Liberar hosts).
5. Escolha Release (Liberar) para confirmar.

AWS CLI

Como liberar um Host dedicado

Use o comando [release-hosts](#) da AWS CLI.

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

Como liberar um Host dedicado

Use o comando [Remove-EC2Hosts](#) do AWS Tools for Windows PowerShell.

```
PS C:\> Remove-EC2Hosts -HostId h-012a3456b7890cdef
```

Depois de liberar um Host dedicado, você não pode reutilizar o mesmo host ou ID de host, e não terá mais taxas de faturamento sob demanda cobradas para ele. O estado do Host dedicado será alterado para `released` e não será mais possível executar nenhuma instância nesse host.

Note

Se você tiver liberado o Hosts dedicados recentemente, poderá levar um tempo para que eles parem de contar para seu limite. Durante esse tempo, você pode receber erros de `LimitExceeded` ao tentar alocar novos Hosts dedicados. Se esse for o caso, tente alocar novos hosts novamente após alguns minutos.

As instâncias que foram interrompidas ainda estão disponíveis para uso e estão listadas na página Instances (Instâncias). Elas retêm sua configuração de alocação de host.

Comprar Reservas de hosts dedicados

É possível comprar reservas usando os seguintes métodos:

Console

Como comprar reservas

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione Hosts dedicados, Reservas de hosts dedicados, Purchase Reserva de hosts dedicados (Comprar Reserva de hosts dedicados).
3. Na tela Purchase Reserva de hosts dedicados (Comprar Reserva de hosts dedicados), é possível pesquisar as ofertas disponíveis usando as configurações padrão ou especificar valores personalizados para o seguinte:
 - Host instance family (Família de instâncias de host) — as opções relacionadas correspondem aos Hosts dedicados de sua conta que não são atribuídos a uma reserva.
 - Availability Zone (Zona de disponibilidade) — a zona de disponibilidade dos Hosts dedicados em sua conta que não são atribuídos a uma reserva.
 - Payment option (Opção de pagamento) — a opção de pagamento da oferta.
 - Term (Período de vigência) — O período de vigência da reserva, que pode ser de um ou três anos.
4. Escolha Find offering (Encontrar oferta) e selecione uma oferta que corresponda às suas necessidades.
5. Escolha os Hosts dedicados a serem associados com a reserva e escolha Review (Revisar).
6. Revise seu pedido e selecione Order (Fazer pedido).

AWS CLI

Como comprar reservas

1. Use o comando [describe-host-reservation-offerings](#) da AWS CLI para listar as ofertas disponíveis que atendam às suas necessidades. O exemplo a seguir lista as ofertas compatíveis com instâncias na família de instâncias m4 e tem período de vigência de um ano.

Note

O prazo é especificado em segundos. Um período de vigência de um ano inclui 31.536.000 segundos, e um período de vigência de três anos inclui 94.608.000 segundos.

```
aws ec2 describe-host-reservation-offerings --filter Name=instance-family,Values=m4  
--max-duration 31536000
```

O comando retorna uma lista de ofertas que correspondem aos seus critérios. Observe o offeringId da oferta a ser comprada.

2. Use o comando [purchase-host-reservation](#) da AWS CLI para comprar a oferta e fornecer o offeringId indicado na etapa anterior. No exemplo a seguir, é comprada a reserva especificada e ela é associada a um Host dedicado específico já atribuído à conta da AWS, cuja tag é aplicada com uma chave de purpose e um valor de production.

```
aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --  
host-id-set h-013abcd2a00cbd123 --tag-specifications 'ResourceType=host-  
reservation,Tags={Key=purpose,Value=production}'
```

PowerShell

Como comprar reservas

1. Use o comando [Get-EC2HostReservationOffering](#) do AWS Tools for Windows PowerShell para listar as ofertas disponíveis que atendam às suas necessidades. Os seguintes exemplos listam as ofertas compatíveis com instâncias na família de instâncias m4 e têm prazo de um ano.

Note

O prazo é especificado em segundos. Um período de vigência de um ano inclui 31.536.000 segundos, e um período de vigência de três anos inclui 94.608.000 segundos.

```
PS C:\> $filter = @{Name="instance-family"; Value="m4"}
```

```
PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
```

O comando retorna uma lista de ofertas que correspondem aos seus critérios. Observe o offeringId da oferta a ser comprada.

2. Use o comando [New-EC2HostReservation](#) do AWS Tools for Windows PowerShell para comprar a oferta e fornecer o offeringId indicado na etapa anterior. No exemplo a seguir, é comprada a reserva especificada e ela é associada a um host dedicado específico já atribuído à conta da AWS.

```
PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -  
HostIdSet h-013abcd2a00cbd123
```

Visualizar reservas de Host dedicado

É possível ver as informações sobre o Hosts dedicados que estão associadas à sua reserva, como:

- O período de vigência da reserva
- A opção de pagamento
- As datas de início e fim

É possível visualizar detalhes de suas reservas do Host dedicado usando os métodos a seguir.

Console

Como ver os detalhes de uma reserva do Host dedicado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Hosts dedicados no painel de navegação.
3. Na página Hosts dedicados, escolha Host dedicado Reservations (Reservas de hosts dedicados) e selecione a reserva na lista fornecida.
4. Selecione Details (Detalhes) para obter informações sobre a reserva.
5. Selecione Hosts para obter informações sobre os Hosts dedicados aos quais a reserva está associada.

AWS CLI

Como ver os detalhes de uma reserva do Host dedicado

Use o comando [describe-host-reservations](#) da AWS CLI.

```
aws ec2 describe-host-reservations
```

PowerShell

Como ver os detalhes de uma reserva do Host dedicado

Use o comando [Get-EC2HostReservation](#) do AWS Tools for Windows PowerShell.

```
PS C:\> Get-EC2HostReservation
```

Atribuir tag de Reservas de hosts dedicados

Você pode atribuir tags personalizadas aos Reservas de hosts dedicados para categorizá-los de diferentes maneiras, como por objetivo, proprietário ou ambiente. Isso ajuda a localizar rapidamente um Reserva de hosts dedicados específico com base na tags personalizadas que você atribuiu.

Só é possível marcar um Reserva de hosts dedicados usando as ferramentas de linha de comando.

AWS CLI

Como marcar um Reserva de hosts dedicados

Use o comando da AWS CLI [create-tags](#).

```
aws ec2 create-tags --resources hr-1234563a4ffc669ae --tags Key=Owner,Value=TeamA
```

PowerShell

Como marcar um Reserva de hosts dedicados

Use o comando do AWS Tools for Windows PowerShell [New-EC2Tag](#).

O comando `New-EC2Tag` precisa de um parâmetro `Tag`, que especifica o par de chave e valor a ser usado na tag da Reserva de hosts dedicados. Os comandos a seguir criam o parâmetro de `Tag`.

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag  
PS C:\> $tag.Key = "Owner"  
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource hr-1234563a4ffc669ae -Tag $tag
```

Trabalhar com Hosts dedicados compartilhado

O compartilhamento de Host dedicado permite que proprietários de Host dedicado compartilhem seus hosts dedicados com outras contas da AWS ou em uma organização da AWS. Isso permite criar e gerenciar os hosts dedicados centralmente, e compartilhar o host dedicado entre várias contas da AWS ou em sua organização da AWS.

Nesse modelo, a conta da AWS que possui o host dedicado (proprietária) compartilha-a com outras contas da AWS (consumidores). Os consumidores podem executar instâncias nos Hosts dedicados que são compartilhadas com eles da mesma maneira que executam instâncias em Hosts dedicados alocados em sua própria conta. O proprietário é responsável pelo gerenciamento do Host dedicado e pelas instâncias executadas nele. Os proprietários não podem modificar instâncias que os consumidores executam em Hosts dedicados compartilhados. Os consumidores são responsáveis por gerenciar as instâncias que executam em Hosts dedicados compartilhados com eles. Os consumidores não podem visualizar ou modificar instâncias de propriedade de outros consumidores ou do proprietário do Host dedicado, e não podem modificar os Hosts dedicados que são compartilhados com eles.

Um proprietário de Host dedicado pode compartilhar um Host dedicado com:

- Contas específicas da AWS dentro ou fora de sua organização na AWS
- Uma unidade organizacional dentro de sua organização da AWS
- Toda a sua organização da AWS

Tópicos

- [Pré-requisitos para compartilhar Hosts dedicados \(p. 374\)](#)
- [Limitações para compartilhamento de Host dedicado \(p. 374\)](#)
- [Serviços relacionados \(p. 374\)](#)
- [Compartilhamento entre zonas de disponibilidade \(p. 374\)](#)
- [Compartilhar um Host dedicado \(p. 374\)](#)
- [Descompartilhar um Host dedicado compartilhado \(p. 375\)](#)
- [Identificar um Host dedicado compartilhado \(p. 376\)](#)
- [Visualizar instâncias em execução em um Host dedicado compartilhado \(p. 377\)](#)
- [Permissões de Host dedicado compartilhado \(p. 377\)](#)
- [Faturamento e medição \(p. 377\)](#)
- [Limites de Host dedicado \(p. 378\)](#)
- [Recuperação de host e compartilhamento do Host dedicado \(p. 378\)](#)

Pré-requisitos para compartilhar Hosts dedicados

- Para compartilhar um host dedicado, é necessário ser o proprietário dele em sua conta da AWS. Não é possível compartilhar um Host dedicado que tenha sido compartilhado com você.
- Para compartilhar um host dedicado com a sua organização da AWS ou com uma unidade organizacional de sua organização da AWS, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte [Enable Sharing with AWS Organizations \(Habilitar o compartilhamento com o AWS Organizations\)](#) no AWS RAM User Guide (Manual do usuário do AWS RAM).

Limitações para compartilhamento de Host dedicado

Não é possível compartilhar Hosts dedicados que foram alocados para os seguintes tipos de instância: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` e `u-24tb1.metal`.

Serviços relacionados

AWS Resource Access Manager

O compartilhamento de host dedicado integra-se ao AWS Resource Access Manager (AWS RAM). O AWS RAM é um serviço que permite compartilhar seus recursos da AWS com qualquer conta da AWS ou por meio do AWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização do AWS Organizations.

Para obter mais informações sobre o AWS RAM, consulte o [Manual do usuário do AWS RAM](#).

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para identificar o local de seus Hosts dedicados relativo a suas contas, use o ID da zona de disponibilidade (ID da AZ). O ID da zona de disponibilidade é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um ID de zona de disponibilidade da região `us-east-1` e é o mesmo local em cada conta da AWS.

Como visualizar os IDs de zona de disponibilidade para as zonas de disponibilidade em sua conta

1. Abra o console do AWS RAM em <https://console.aws.amazon.com/ram>.
2. Os IDs de zona de disponibilidade da região atual são exibidos no painel Your AZ ID (Seu ID de AZ) no lado direito da tela.

Compartilhar um Host dedicado

Quando um proprietário compartilha um Host dedicado, ele permite que os consumidores executem instâncias no host. Os consumidores podem executar tantas instâncias no host compartilhado quanto sua capacidade disponível permitir.

Important

Observe que você é responsável por garantir que possui direitos de licença apropriados para compartilhar qualquer licença BYOL no Hosts dedicados.

Se você compartilhar um Host dedicado com o posicionamento automático habilitado, lembre-se do seguinte, pois isso pode gerar uso não intencional do Host dedicado:

- Se os consumidores executarem instâncias com locação de Host dedicado e não tiverem capacidade em um Host dedicado que possuam na conta, a instância será executada automaticamente no Host dedicado compartilhado.

Para compartilhar um Host dedicado, é necessário adicioná-lo a um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Você pode adicionar o Host dedicado a um recurso existente ou adicioná-lo a um novo compartilhamento de recursos.

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na organização, os consumidores da organização receberão acesso automaticamente ao host dedicado compartilhado. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e acesso ao Host dedicado compartilhado depois de aceitar o convite.

Note

Depois de compartilhar um Host dedicado, pode levar alguns minutos para que os consumidores tenham acesso a ele.

Você pode compartilhar um Host dedicado de sua propriedade usando um dos seguintes métodos.

Amazon EC2 console

Como compartilhar um Host dedicado de sua propriedade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Escolha o Host dedicado a ser compartilhado e selecione Ações, Compartilhar host.
4. Selecione o compartilhamento de recursos ao qual adicionar o Host dedicado e escolha Compartilhar host.

Pode levar alguns minutos para que os consumidores obtenham acesso ao host compartilhado.

AWS RAM console

Como compartilhar um host dedicado de sua propriedade usando o console do AWS RAM

Consulte [Criar um compartilhamento de recursos](#) no Manual do usuário do AWS RAM.

AWS CLI

Para compartilhar um host dedicado de sua propriedade usando a AWS CLI

Use o comando [create-resource-share](#).

Descompartilhar um Host dedicado compartilhado

O proprietário do Host dedicado pode cancelar o compartilhamento de um Host dedicado compartilhado a qualquer momento. Ao cancelar o compartilhamento de um Host dedicado compartilhado, as seguintes regras são aplicadas:

- Os consumidores com os quais o Host dedicado foi compartilhado não podem mais executar novas instâncias nele.

- As instâncias de propriedade de consumidores que estavam em execução no Host dedicado no momento do cancelamento do compartilhamento continuam a ser executadas, mas são programadas para [desativação](#). Os consumidores recebem notificações de desativação para as instâncias e têm duas semanas para agir sobre as notificações. No entanto, se o Host dedicado for compartilhado novamente com o consumidor durante o período de aviso de desativação, as desativações de instância serão canceladas.

Para cancelar o compartilhamento de um Host dedicado compartilhado de sua propriedade, é necessário removê-lo do compartilhamento de recursos. Isso pode ser feito usando um dos seguintes métodos.

Amazon EC2 console

Como cancelar o compartilhamento de um Host dedicado compartilhado de sua propriedade usando o console do Amazon EC2

- Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
- No painel de navegação, selecione Hosts dedicados.
- Escolha o Host dedicado do qual cancelar o compartilhamento e escolha a guia Compartilhamento.
- A guia Compartilhamento lista os compartilhamentos de recursos aos quais o Host dedicado foi adicionado. Selecione o compartilhamento de recursos do qual remover o Host dedicado e escolha Remover do compartilhamento de recursos.

AWS RAM console

Como cancelar o compartilhamento de um host dedicado compartilhado de sua propriedade usando o console do AWS RAM

Consulte [Updating a Resource Share \(Atualização de um compartilhamento de recursos\)](#) no AWS RAM User Guide (Manual do usuário do AWS RAM).

Command line

Para cancelar o compartilhamento de um host dedicado compartilhado de sua propriedade usando a AWS CLI

Use o comando [disassociate-resource-share](#).

Identificar um Host dedicado compartilhado

Proprietários e consumidores podem identificar Hosts dedicados compartilhados usando um dos seguintes métodos.

Amazon EC2 console

Como identificar um Host dedicado compartilhado usando o console do Amazon EC2

- Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
- No painel de navegação, selecione Hosts dedicados. A tela lista Hosts dedicados de sua propriedade e Hosts dedicados compartilhados com você. A coluna Owner (Proprietário) mostra o ID de conta da AWS do proprietário do host dedicado.

Command line

Como identificar um host dedicado compartilhado usando a AWS CLI

Use o comando [describe-hosts](#). O comando retorna os Hosts dedicados de sua propriedade e os Hosts dedicados compartilhados com você.

Visualizar instâncias em execução em um Host dedicado compartilhado

Proprietários e consumidores podem visualizar as instâncias em execução em um Host dedicado compartilhado a qualquer momento usando um dos seguintes métodos.

Amazon EC2 console

Como visualizar as instâncias em execução em um Host dedicado compartilhado usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado para o qual deseja visualizar as instâncias e escolha Instances (Instâncias). A guia lista as instâncias em execução no host. Os proprietários veem todas as instâncias em execução no host, incluindo instâncias executadas pelos consumidores. Os consumidores veem somente as instâncias que executaram no host. A coluna Owner (Proprietário) mostra o ID da conta da AWS que executou a instância.

Command line

Como visualizar as instâncias em execução em um host dedicado compartilhado usando a AWS CLI

Use o comando [describe-hosts](#). O comando retorna as instâncias em execução em cada Host dedicado. Os proprietários veem todas as instâncias em execução no host. Os consumidores veem somente as instâncias em execução que executaram nos hosts compartilhados. `InstanceOwnerId` mostra o ID de conta da AWS do proprietário da instância.

Permissões de Host dedicado compartilhado

Permissões para proprietários

Os proprietários são responsáveis pelo gerenciamento de seus Hosts dedicados compartilhados e das instâncias executadas neles. Os proprietários podem visualizar todas as instâncias em execução no Host dedicado compartilhado, incluindo aquelas executadas pelos consumidores. No entanto, os proprietários não podem realizar ações nas instâncias que foram executadas pelos consumidores.

Permissões para consumidores

Os consumidores são responsáveis por gerenciar as instâncias que executam em um Host dedicado compartilhado. Os consumidores não podem modificar o Host dedicado compartilhado de nenhuma forma e não podem visualizar nem modificar instâncias que foram executadas por outros consumidores ou pelo proprietário do Host dedicado.

Faturamento e medição

Não há cobranças adicionais pelo compartilhamento de Hosts dedicados.

Os proprietários são cobrados por Hosts dedicados compartilhado. Os consumidores não são cobrados pelas instâncias que executam no Hosts dedicados compartilhado.

Reservas de hosts dedicados continuam a oferecer descontos de cobrança por Hosts dedicados compartilhados. Somente proprietários de Host dedicado podem comprar Reservas de hosts dedicados para Hosts dedicados compartilhados que possuem.

Limites de Host dedicado

Hosts dedicados compartilhados são contabilizados somente para os limites de Hosts dedicados do proprietário. Os limites de Hosts dedicados do consumidor não são afetados por Hosts dedicados que foram compartilhados com eles. Da mesma forma, as instâncias executadas pelos consumidores em Hosts dedicados compartilhados não são contabilizadas para seus limites de instâncias.

Recuperação de host e compartilhamento do Host dedicado

A recuperação de host recupera instâncias executadas pelo proprietário do Host dedicado e pelos consumidores com os quais ele foi compartilhado. O Host dedicado de reposição é alocado na conta do proprietário. É adicionado aos mesmos compartilhamentos de recursos que o Host dedicado original e é compartilhado com os mesmos consumidores.

Para obter mais informações, consulte [Recuperação do host \(p. 378\)](#).

Recuperação do host

A recuperação do host reinicia automaticamente suas instâncias para um novo host de substituição se forem detectadas falhas no seu Host dedicado. A recuperação do host reduz a necessidade de intervenção manual e diminui o fardo operacional se houver falha inesperada no Host dedicado.

Além disso, a integração incorporada com o AWS License Manager automatiza o monitoramento e o gerenciamento das suas licenças, caso ocorra uma recuperação do host.

Note

A integração com o AWS License Manager é compatível somente nas regiões em que o AWS License Manager está disponível.

Tópicos

- [Conceitos básicos de recuperação do host \(p. 378\)](#)
- [Tipos de instâncias compatíveis \(p. 379\)](#)
- [Configurar a recuperação do host \(p. 379\)](#)
- [Estados de recuperação do host \(p. 381\)](#)
- [Recuperar manualmente instâncias incompatíveis \(p. 381\)](#)
- [Serviços relacionados \(p. 382\)](#)
- [Pricing \(p. 382\)](#)

Conceitos básicos de recuperação do host

A recuperação do host usa verificações de integridade no nível do host para avaliar a disponibilidade do host dedicado e detectar falhas subjacentes no sistema. Os exemplos de problemas que podem causar falha nas verificações de integridade no nível do host incluem:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de hardware ou software no host físico

Ao detectar uma falha no sistema no seu Host dedicado, a recuperação do host é iniciada e o Amazon EC2 aloca automaticamente um Host dedicado em substituição. O Host dedicado em substituição recebe um novo ID do host, mas retém os mesmos atributos que o Host dedicado original, como:

- Availability Zone
- Tipo de instância

- Tags
- Configurações de autoposicionamento

Depois de o Host dedicado de substituição ser alocado, as instâncias serão recuperadas para o Host dedicado de substituição. As instâncias recuperadas retêm os mesmos atributos que as instâncias originais, como:

- ID da instância
- Endereços IP privados
- Endereços IP elásticos
- Anexos de volume do EBS
- Todos os metadados da instância

Se as instâncias tiverem um relacionamento de afinidade de host com o Host Dedicado prejudicado, as instâncias recuperadas estabelecem afinidade do host com o Host Dedicado de substituição.

Quando todas as instâncias tiverem sido recuperadas para o Host dedicado de substituição, o Host dedicado prejudicado será liberado e o Host dedicado de substituição ficará disponível para uso.

Quando a recuperação do host for iniciada, o proprietário da conta da AWS será notificado por e-mail e por um evento AWS Personal Health Dashboard. A segunda notificação é enviada após a recuperação do host ser concluída com sucesso.

As instâncias interrompidas não são recuperadas para o Host dedicado de substituição. Se você tentar iniciar uma instância interrompida que mire no Host dedicado prejudicado, o início da instância falhará. Recomendamos que você modifique a instância interrompida para mirar em um Host Dedicado diferente ou abrir em qualquer Host Dedicado disponível, com configurações correspondentes e autoposicionamento habilitado.

As instâncias com armazenamento de instâncias não são recuperadas para o Host dedicado de substituição. Como medida de remediação, o Host dedicado prejudicado será marcado para desativação e você receberá tal notificação depois de a recuperação do host ser concluída. Siga as etapas de remediação descritas na notificação de desativação dentro do prazo especificado para recuperar manualmente as instâncias restantes no Host dedicado prejudicado.

Se você estiver usando o AWS License Manager para acompanhar suas licenças, o AWS License Manager alocará novas licenças para o host dedicado de substituição conforme os limites de configuração da licença. Se a configuração da licença tiver limites que serão violados como resultado da recuperação do host, o processo de recuperação não será permitido e você será notificado acerca da falha de recuperação do host por meio de uma notificação do Amazon SNS. Se a configuração da licença tiver limites suaves que serão violados como resultado da recuperação do host, a recuperação poderá continuar e você será notificado acerca da violação do limite por meio de uma notificação do Amazon SNS. Para obter mais informações, consulte [Usar configurações de licença](#) no AWS Manual do usuário do AWS License Manager.

Tipos de instâncias compatíveis

A recuperação do host tem suporte para as seguintes famílias de instâncias: A1, C3, C4, C5, C5n, M3, M4, M5, M5n, P3, R3, R4, R5, R5n, X1, X1e, u-6tb1, u-9tb1, u-12tb1, u-18tb1 e u-24tb1.

Para recuperar instâncias não compatíveis, consulte [Recuperar manualmente instâncias incompatíveis \(p. 381\)](#).

Configurar a recuperação do host

Você pode configurar a recuperação do host no momento da alocação do Host dedicado ou após a alocação, usando o console do Amazon EC2 ou a AWS Command Line Interface (CLI).

Tópicos

- [Ativar a recuperação do host \(p. 380\)](#)
- [Desativar a recuperação do host \(p. 380\)](#)
- [Visualizar a configuração de recuperação do host \(p. 380\)](#)

Ativar a recuperação do host

Você pode habilitar a recuperação do host no momento da alocação do Host dedicado ou após a alocação.

Para obter mais informações sobre como habilitar a recuperação do host no momento da alocação do Host dedicado, consulte [Alocar Hosts dedicados \(p. 355\)](#).

Como habilitar a recuperação do host após a alocação usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado para o qual habilitar a recuperação do host e escolha Actions (Ações), Modify Host Recovery (Modificar recuperação do host).
4. Para Host recovery (Recuperação do host), selecione Enable (Habilitar) e Save (Salvar).

Como habilitar a recuperação do host após a alocação usando a AWS CLI

Use o comando [modify-hosts](#) e especifique o parâmetro `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery on --host-ids h-012a3456b7890cdef
```

Desativar a recuperação do host

Você pode desabilitar a recuperação do host a qualquer momento após o Host dedicado ser alocado.

Como desabilitar a recuperação do host após a alocação usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado no qual a recuperação do host será desabilitada e escolha Actions (Ações), Modify Host Recovery (Modificar recuperação do host).
4. Para Host recovery (Recuperação do host), selecione Disable (Desabilitar) e Save (Salvar).

Como desabilitar a recuperação do host após a alocação usando a AWS CLI

Use o comando [modify-hosts](#) e especifique o parâmetro `host-recovery`.

```
$ aws ec2 modify-hosts --host-recovery off --host-ids h-012a3456b7890cdef
```

Visualizar a configuração de recuperação do host

Você pode ver a configuração de recuperação do host para o Host dedicado a qualquer momento.

Como visualizar a configuração de recuperação do host para um Host dedicado usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Hosts dedicados.
3. Selecione o Host dedicado e, na aba Description (Descrição), confira o campo Host Recovery (Recuperação do host).

Como visualizar a configuração de recuperação do host para um Host dedicado usando a AWS CLI

Use o comando [describe-hosts](#).

```
$ aws ec2 describe-hosts --host-ids h-012a3456b7890cdef
```

O elemento de resposta do `HostRecovery` indica se a recuperação do host está habilitada ou desabilitada.

Estados de recuperação do host

Quando a falha do Host dedicado for detectada, o Host dedicado prejudicado entra no estado `under-assessment` e todas as instâncias entram no estado `impaired`. Não é possível executar instâncias no Host dedicado prejudicado enquanto estiver no estado `under-assessment`.

Depois de o Host dedicado de substituição ser alocado, ele entra no estado `pending`. Ele continua nesse estado até que o processo de recuperação do host esteja concluído. Não é possível executar instâncias no Host dedicado de substituição enquanto ele estiver no estado `pending`. As instâncias recuperadas no Host dedicado de substituição continuam no estado `impaired` durante o processo de recuperação.

Depois de a recuperação do host ser concluída, o Host dedicado de substituição entrará no estado `available` e as instâncias recuperadas retornarão ao estado `running`. Você pode abrir instâncias no Host dedicado de substituição depois de entrar no estado `available`. O Host dedicado prejudicado original é liberado permanentemente e entra no estado `released-permanent-failure`.

Se o Host dedicado prejudicado tiver instâncias incompatíveis com a recuperação do host, como instâncias com volumes compatíveis com o armazenamento de instâncias, o Host dedicado não será liberado. Em vez disso, é marcado para aposentadora e entra no estado `permanent-failure`.

Recuperar manualmente instâncias incompatíveis

A recuperação do host não é compatível com a recuperação de instâncias que usam volumes do armazenamento de instâncias. Siga as instruções abaixo para recuperar à mão todas as instâncias que não puderem ser recuperadas automaticamente.

Warning

Os dados nos volumes de armazenamento de instâncias serão perdidos quando a instância for interrompida, hibernada ou encerrada. Isso inclui volumes de armazenamento de instância anexados a uma instância que possui um volume do EBS como dispositivo raiz. Para proteger os dados dos volumes de armazenamento de instâncias, faça backup no armazenamento persistente antes de a instância ser interrompida ou encerrada.

Recuperar manualmente instâncias compatíveis com EBS

Para instâncias compatíveis com EBS que não possam ser recuperadas automaticamente, recomendamos pará-las e iniciá-las automaticamente para recuperá-las a um novo Host dedicado. Para obter mais informações sobre como interromper a instância, além de informações sobre as mudanças em sua configuração de instância quando ela estiver interrompida, consulte [Interromper e iniciar sua instância \(p. 455\)](#).

Recuperar manualmente instâncias compatíveis com armazenamento de instâncias

Para instâncias compatíveis com armazenamento de instâncias que não possam ser automaticamente recuperadas, recomendamos fazer o seguinte:

1. Abrir a instância de substituição em um novo Host dedicado a partir da AMI mais recente.
2. Migrar todos os dados necessários para a instância de substituição.
3. Encerrar a instância original no Host dedicado prejudicado.

Serviços relacionados

O Host dedicado se integra com os seguintes serviços:

- AWS License Manager: monitora licenças em seus hosts dedicados do Amazon EC2 (compatível somente nas regiões em que o AWS License Manager está disponível). Para obter mais informações, consulte o [AWS Manual do usuário do AWS License Manager](#).

Pricing

Não há cobranças adicionais para usar a recuperação do host; aplicam-se as cobranças usuais do Host dedicado. Para obter mais informações, consulte [Definição de preço de hosts dedicados do Amazon EC2](#).

Assim que a recuperação for iniciada, você não será mais cobrado pelo Host dedicado prejudicado. A cobrança pelo host dedicado começa somente depois de entrar no estado `available`.

Se o Host dedicado prejudicado tiver sido cobrado usando a taxa sob demanda, o Host dedicado de substituição também são cobrados usando essa taxa. Se o Host dedicado prejudicado tiver um Reserva de hosts dedicados ativo, ele será transferido para o Host dedicado de substituição.

Monitorar alterações de configuração

Você pode usar o AWS Config para gravar as alterações de configuração de hosts dedicados e de instâncias que são executadas, interrompidas ou encerradas neles. Em seguida, use as informações capturadas pelo AWS Config como fonte de dados para geração de relatórios de licenças.

O AWS Config grava individualmente as informações de configuração dos hosts dedicados e das instâncias e emparelha essas informações por meio de relacionamentos. Há três condições de geração de relatórios:

- AWS Config recording status (Status de gravação do AWS Config): quando On (Ativado), o AWS Config está gravando um ou mais tipos de recursos da AWS que podem incluir hosts dedicados e instâncias dedicadas. Para capturar as informações necessárias para geração de relatórios de licenças, verifique se os hosts e as instâncias estão sendo gravados com os campos a seguir.
- Status de gravação do host — quando está Enabled (Habilitado), as informações de configuração de Hosts dedicados são gravadas.
- Instance recording status (Status de gravação da instância) — quando Enabled (Habilitado), as informações de configuração de Instâncias dedicadas são gravadas.

Se qualquer uma das três condições estiver desabilitada, o ícone do botão Edit Config Recording (Editar gravação de configuração) ficará vermelho. Para aproveitar todos os benefícios dessa ferramenta, verifique se os três métodos de gravação estão ativados. Quando os três estão ativados, o ícone fica verde. Para editar as configurações, escolha Edit Config Recording (Editar gravação de configuração). Você será direcionado à pagina Set up AWS Config (Configurar CC) no console do AWS Config, onde poderá configurar o AWS Config e começar a gravar em seus hosts, instâncias e outros tipos de recursos com suporte. Para obter mais informações, consulte [Configuração do AWS Config para uso do console](#) no Guia do desenvolvedor do AWS Config.

Note

AWS Config grava seus recursos depois de descobri-los, o que pode levar vários minutos.

Depois que o AWS Config começa a gravar alterações de configuração nos hosts e nas instâncias, você obtém o histórico de configuração de qualquer host que tenha alocado ou liberado e qualquer instância que tenha executado, interrompido ou encerrado. Por exemplo, a qualquer momento no histórico de configuração de um Host dedicado, você pode pesquisar quantas instâncias são executadas nesse

host, juntamente com o número de soquetes e núcleos no host. Para qualquer uma dessas instâncias, você também pode procurar o ID de sua imagem de máquina da Amazon (AMI). Você pode usar essas informações para gerar relatórios de licenças para seu próprio software ligado ao servidor, que é licenciado por soquete ou por núcleo.

É possível visualizar os históricos de configuração de qualquer uma destas maneiras:

- Usando o console do AWS Config. Para cada recursos gravado, você pode visualizar uma página de linha do tempo, que fornece o histórico com detalhes de configuração. Para visualizar essa página, escolha o ícone cinza na coluna Config Timeline (Configurar linha de tempo) da página Hosts dedicados. Para obter mais informações, consulte [Visualização de detalhes de configuração do console do AWS Config](#) no Guia do desenvolvedor do AWS Config.
- Executando comandos da AWS CLI. Primeiro, você pode usar o comando `list-discovered-resources` para obter uma lista de todos os hosts e instâncias. Depois, você pode usar o comando `get-resource-config-history` para obter detalhes de configuração de um host ou instância para um intervalo de tempo específico. Para obter mais informações, consulte [Visualização de detalhes de configuração usando a CLI](#) no Guia do desenvolvedor do AWS Config.
- Usando a API do AWS Config em suas aplicações. Primeiro, você pode usar a ação `ListDiscoveredResources` para obter uma lista de todos os hosts e instâncias. Depois, você pode usar a ação `GetResourceConfigHistory` para obter detalhes de configuração de um host ou instância para um intervalo de tempo específico.

Por exemplo, para obter uma lista de todos os hosts dedicados do AWS Config, execute um comando da CLI como o a seguir.

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Para obter o histórico de configurações de um host dedicado do AWS Config, execute um comando da CLI como o a seguir.

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --  
resource-id i-1234567890abcdef0
```

Para gerenciar as configurações do AWS Config usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na página Hosts dedicados, escolha Edit Config Recording (Editar gravação de configuração).
3. No console do AWS Config, siga as etapas fornecidas para ativar a gravação. Para obter mais informações, consulte [Configuração do AWS Config usando o console](#).

Para obter mais informações, consulte [Visualização de detalhes de configuração no console do AWS Config](#).

Como ativar o AWS Config usando a linha de comando ou a API

- CLI da AWS: [Visualizar detalhes da configuração \(AWS CLI\)](#) no Guia do desenvolvedor do AWS Config.
- API do Amazon EC2: [GetResourceConfigHistory](#).

Dedicated Instances

Instâncias dedicadas são instâncias do Amazon EC2 que são executadas em uma nuvem privada virtual (VPC) em um hardware dedicado a um único cliente. As instâncias dedicadas que pertencem a diferentes contas da AWS são isoladas fisicamente em nível de hardware, mesmo que essas contas

estejam vinculadas a uma única conta pagante. No entanto, as instâncias dedicadas podem compartilhar o hardware com outras instâncias da mesma conta da AWS que não sejam instâncias dedicadas.

Note

Um Host dedicado também é um servidor físico que é dedicado para seu uso. Com um Host dedicado, você tem visibilidade e controle sobre como as instâncias são colocadas no servidor. Para obter mais informações, consulte [Dedicated Hosts \(p. 349\)](#).

Tópicos

- [Conceitos básicos da Instâncias dedicadas \(p. 384\)](#)
- [Recursos compatíveis \(p. 384\)](#)
- [Diferenças entre instâncias dedicadas e hosts dedicados \(p. 386\)](#)
- [Limitações da Instâncias dedicadas \(p. 386\)](#)
- [Definição de preço para Instâncias dedicadas \(p. 386\)](#)
- [Como trabalhar com Instâncias dedicadas \(p. 387\)](#)

Conceitos básicos da Instâncias dedicadas

Instâncias dedicadas só podem ser iniciadas em uma Amazon VPC.

Quando você inicia uma instância, o atributo de locação da instância determina o hardware no qual ela é executada. Para iniciar uma instância dedicada, é necessário especificar uma locação de instância de dedicated.

Note

Instâncias com um valor de locação de default são executadas em hardware de locação compartilhada. Instâncias com um valor de locação de host são executadas em um Host Dedicado. Para obter mais informações sobre como trabalhar com hosts dedicados, consulte [Dedicated Hosts \(p. 349\)](#).

A locação da VPC na qual você inicia a instância também pode determinar a locação da instância. Uma VPC pode ter uma locação de default ou dedicated. Se você iniciar uma instância em uma VPC que tenha uma locação de default, a instância é executada, por padrão, em hardware de locação compartilhada, a menos que você especifique outra locação para a instância. Se você iniciar uma instância em uma VPC que tenha uma locação de dedicated, a instância é executada, por padrão, como uma instância dedicada, a menos que você especifique outra locação para a instância.

Para iniciar instâncias dedicadas, você pode fazer o seguinte:

- Crie uma VPC com uma locação de dedicated e inicie todas as instâncias como instâncias dedicadas por padrão. Para obter mais informações, consulte [Criação de uma VPC com uma locação de instância dedicada \(p. 387\)](#).
- Crie uma VPC com uma locação de default e especifique manualmente uma locação de dedicated para as instâncias que você deseja executar como instâncias dedicadas. Para obter mais informações, consulte [Executar Instâncias dedicadas em um VPC \(p. 387\)](#).

Recursos compatíveis

Instâncias dedicadas são compatíveis com os seguintes recursos e integrações de serviço da AWS:

Tópicos

- [Reserved Instances \(p. 385\)](#)

- Escalabilidade automática (p. 385)
- Recuperação automática (p. 385)
- Instâncias spot dedicadas (p. 385)
- Instâncias expansíveis (p. 385)

Reserved Instances

Para garantir que tem capacidade suficiente disponível para executar Instâncias dedicadas, você pode comprar Instâncias reservadas dedicadas. Para obter mais informações, consulte [Reserved Instances \(p. 259\)](#).

Ao adquirir uma Instância reservada dedicada, você estará comprando capacidade de executar uma Instâncias dedicadas em uma VPC a uma taxa de uso muito reduzida. A redução de preço na cobrança de uso se aplica apenas quando você executa uma instância com locação dedicada. Quando você compra uma Instância reservada com locação padrão, ela se aplica somente a uma instância em execução com locação default. Ela não é aplicada a uma instância em execução com locação dedicated.

Você não pode usar o processo de modificação para alterar a locação de uma Instância reservada depois de adquiri-la. No entanto, é possível trocar uma Instância reservada convertível por uma nova Instância reservada convertível com uma locação diferente.

Escalabilidade automática

Você pode usar o Amazon EC2 Auto Scaling para executar Instâncias dedicadas. Para obter mais informações, consulte [Execução de instâncias do Auto Scaling em uma VPC](#) no Guia do usuário do Amazon EC2 Auto Scaling.

Recuperação automática

Você pode configurar a recuperação automática para uma instância dedicada se ela ficar impedida devido a uma falha de hardware subjacente ou a um problema que exija o envolvimento da AWS para ser reparado. Para obter mais informações, consulte [Recuperar a instância \(p. 480\)](#).

Instâncias spot dedicadas

Você pode executar uma instância spot dedicada especificando uma locação de dedicated ao criar uma solicitação de instâncias spot. Para obter mais informações, consulte [Especificando uma locação para suas Instâncias spot \(p. 311\)](#).

Instâncias expansíveis

É possível aproveitar os benefícios da execução em hardware de locação dedicada com [the section called “Instâncias expansíveis” \(p. 169\)](#). As instâncias dedicadas T3 são executadas no modo ilimitado por padrão, e elas fornecem um nível de linha de base de performance da CPU com a capacidade de intermitência para um nível de CPU mais alto quando exigido por sua workload. A performance basal da T3 e a capacidade de intermitência são regidas por créditos de CPU. Devido à natureza intermitente dos tipos de instância T3, recomendamos monitorar como suas instâncias T3 usam os recursos de CPU do hardware dedicado para obter a melhor performance. As instâncias dedicadas T3 destinam-se a clientes com workloads diversas que exibem comportamento aleatório da CPU, mas que, preferencialmente, têm o uso médio da CPU em ou abaixo dos usos da linha de base. Para obter mais informações, consulte [the section called “Principais conceitos” \(p. 171\)](#).

O Amazon EC2 tem sistemas para identificar e corrigir a variabilidade na performance. No entanto, ainda é possível passar por variabilidade de curto prazo se você iniciar várias instâncias dedicadas T3 que tenham padrões correlacionados de uso da CPU. Para essas workloads mais exigentes ou correlacionadas, recomendamos o uso de instâncias dedicadas M5 ou M5a em vez de instâncias dedicadas T3.

Diferenças entre instâncias dedicadas e hosts dedicados

Instâncias dedicadas e hosts dedicados podem ser usados para iniciar instâncias do Amazon EC2 em servidores físicos que são dedicados para seu uso.

Não há diferenças físicas de performance ou de segurança entre Instâncias dedicadas e instâncias em Hosts dedicados. No entanto, existem algumas diferenças entre os dois. A tabela a seguir destaca algumas das principais diferenças entre Hosts dedicados e Instâncias dedicadas:

	Dedicated Host	Dedicated Instance
Faturamento	faturamento por host	Faturamento por instância
Visibilidade de soquetes, núcleos e ID de host	Fornece visibilidade do número de soquetes e núcleos físicos no host	Sem visibilidade
Afinidade de hosts e instâncias	Permite implantar de forma consistente suas instâncias no mesmo host físico ao longo do tempo	Sem suporte
Posicionamento direcionado de instâncias	Fornece controle sobre como as instâncias são colocadas no host	Sem suporte
Recuperação automática de instâncias	Compatível	Compatível
Traga sua própria licença (BYOL)	Compatível	Sem suporte

Para obter mais informações sobre hosts dedicados, consulte [Dedicated Hosts \(p. 349\)](#).

Limitações da Instâncias dedicadas

Tenha o seguinte em mente ao usar Instâncias dedicadas:

- Alguns serviços da AWS ou seus recursos não são compatíveis com uma VPC com a locação de instância definida como `dedicated`. Verifique a documentação do serviço para confirmar se há alguma limitação.
- Alguns tipos de instância não podem ser iniciados em uma VPC com a locação da instância definida como `dedicated`. Para obter mais informações sobre os tipos de instância compatíveis, consulte [Instâncias dedicadas do Amazon EC2](#).
- Quando você iniciar uma instância dedicada compatível com o Amazon EBS, o volume do EBS não é executado em hardware de ocupante único.

Definição de preço para Instâncias dedicadas

A definição de preço de Instâncias dedicadas é diferente da definição de preço de Instâncias sob demanda. Para obter mais informações, consulte a [página do produto de Instâncias dedicadas do Amazon EC2](#).

Como trabalhar com Instâncias dedicadas

Você pode criar uma VPC com uma locação de instância `dedicated` para garantir que todas as instâncias executadas na VPC sejam Instâncias dedicadas. Como alternativa, você pode especificar a locação da instância durante a execução.

Tópicos

- [Criação de uma VPC com uma locação de instância dedicada \(p. 387\)](#)
- [Executar Instâncias dedicadas em um VPC \(p. 387\)](#)
- [Exibir informações de locação \(p. 388\)](#)
- [Altere a locação de uma instância \(p. 389\)](#)
- [Alterar a locação de uma VPC \(p. 390\)](#)

Criação de uma VPC com uma locação de instância dedicada

Ao criar uma VPC, você tem a opção de especificar sua locação de instância. Se você estiver usando o console da Amazon VPC, poderá criar uma VPC usando o assistente de VPC ou a página Your VPCs (Suas VPCs).

Se você executar uma instância em uma VPC que tem uma locação de instância `dedicated`, sua instância será automaticamente uma Instâncias dedicadas, independentemente da locação da instância.

Console

Para criar uma VPC com uma locação de instância de dedicada (Assistente de VPC)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel, selecione Launch VPC Wizard (Iniciar assistente da VPC).
3. Selecione uma configuração de VPC e escolha Select (Selecionar).
4. Para Hardware tenancy (Locação de hardware), escolha Dedicated (Dedicado).
5. Escolha Criar VPC.

Para criar uma VPC com uma locação de instância de dedicada (caixa de diálogo Criar VPC)

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs) e Create VPC (Criar VPC).
3. Em Tenancy (Locação), escolha Dedicated (Dedicada). Especifique o bloco CIDR e escolha Create VPC (Criar VPC).

Command line

Para configurar a opção de locação quando você cria uma VPC usando a linha de comando

- `create-vpc` (AWS CLI)
- `New-EC2Vpc` (AWS Tools for Windows PowerShell)

Executar Instâncias dedicadas em um VPC

Você pode executar uma Instâncias dedicadas usando o assistente de execução de instâncias do Amazon EC2.

Console

Para executar uma Instâncias dedicadas em uma VPC de locação padrão usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Launch Instance (Executar instância).
3. Na página Choose an Amazon Machine Image (AMI) (Escolher uma imagem de máquina da Amazon), selecione uma AMI e escolha Select (Selecionar).
4. Na página Choose an Instance Type (Escolher um tipo de instância), selecione o tipo de instância e escolha Next: Configure Instance Details (Próximo: Configurar os detalhes da instância).

Note

Escolha um tipo de instância que tenha suporte como uma Instâncias dedicadas. Para obter mais informações, consulte [Instâncias dedicadas do Amazon EC2](#).

5. Na página Configure Instance Details (Configurar detalhes da instância), selecione uma VPC e uma sub-rede. Para Tenancy (Locação), escolha Dedicated - Run a dedicated instance(Dedicado - Executar uma instância dedicada) e, em seguida, escolha Next: Add Storage (Próximo: Adicionar armazenamento).
6. Continue como solicitado pelo assistente. Ao terminar de revisar suas opções na página Review Instance Launch (Revisar execução da instância), escolha Launch (Executar) para escolher um par de chaves e executar a Instâncias dedicadas.

Command line

Para configurar a opção de locação para uma instância durante a execução usando a linha de comando

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (AWS Tools for Windows PowerShell)

Para obter mais informações sobre a execução de uma instância com uma locação de host, consulte [Execute instâncias em um Host dedicado. \(p. 357\)](#).

Exibir informações de locação

Console

Para exibir as informações da locação da VPC usando o console

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Verifique a locação da instância de sua VPC na coluna Tenancy (Locação).
4. Se a coluna Locação não for exibida, escolha o ícone de configurações () no canto superior direito, alterne para escolher Locação e escolha Confirmar.

Para exibir as informações da locação da sua instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Verifique a locação da instância na coluna Tenancy (Locação).
4. Se a coluna Tenancy (Locação) não for exibida, faça o seguinte:

- Escolha o ícone de configurações (no canto superior direito, alterne para escolher Locação e escolha Confirmar.
- Selecione a instância. Na guia Details (Detalhes) perto da parte inferior da página, em Host and placement group (Host e grupo de posicionamento), verifique o valor de Tenancy (Locação).

Command line

Para descrever a locação da sua VPC usando a linha de comando

- [describe-vpcs](#) (AWS CLI)
- [Get-EC2Vpc](#) (AWS Tools for Windows PowerShell)

Para descrever a locação da sua instância usando a linha de comando

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (AWS Tools for Windows PowerShell)

Para descrever o valor da locação de uma Instância reservada usando a linha de comando

- [describe-reserved-instances](#) (AWS CLI)
- [Get-EC2ReservedInstance](#) (AWS Tools for Windows PowerShell)

Para descrever o valor da locação de uma oferta de Instância reservada usando a linha de comando

- [describe-reserved-instances-offerings](#) (AWS CLI)
- [Get-EC2ReservedInstancesOffering](#) (AWS Tools for Windows PowerShell)

Altere a locação de uma instância

Você pode alterar a locação de uma instância apenas de `dedicated` para `host` ou de `host` para `dedicated` depois de iniciar. As alterações que fizer entrarão em vigor na próxima vez que a instância for iniciada.

Note

- Você não pode alterar a locação de uma instância de `default` para `dedicated` ou `host` depois de iniciar. E você não pode alterar a locação de uma instância de `dedicated` para `host` ou `default` depois de iniciar.
- Para instâncias T3, você não pode alterar a locação de `dedicated` para `host`, ou de `host` para `dedicated`. A tentativa de fazer uma dessas alterações de locação não compatíveis resulta no código de erro `InvalidTenancy`.

Console

Para alterar a locação de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Escolha Instance state (Estado da instância), Stop instance (Interromper instância), Stop (Interromper).

4. Escolha Actions (Ações), Instance Settings (Configurações da instância) e Modify Instance Placement (Modificar posicionamento da instância).
5. Na lista Tenancy (Locação), escolha se a instância será executada em um hardware dedicado ou em um Host dedicado. Escolha Save (Salvar).

Command line

Para modificar o valor da locação de uma instância usando a linha de comando

- [modify-instance-placement](#) (AWS CLI)
- [Edit-EC2InstancePlacement](#) (AWS Tools for Windows PowerShell)

Alterar a locação de uma VPC

Você pode alterar a locação da instância de uma VPC de `dedicated` para `default` depois de criá-la. Alterar a locação da instância da VPC não afeta a locação de nenhuma instância existente na VPC. Na próxima vez que você executar uma instância na VPC, ela terá a locação `default`, a menos que você especifique o contrário durante a execução.

Note

Você não pode alterar a locação da instância de uma VPC de `default` para `dedicated` depois de criá-la.

Você só pode modificar a locação da instância de uma VPC usando a AWS CLI, um AWS SDK ou a API do Amazon EC2.

Command line

Para modificar o atributo de locação da instância de uma VPC usando a AWS CLI

Use o comando [modify-vpc-tenancy](#) e especifique o ID da VPC e o valor da locação da instância. O único valor suportado é `default`.

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

On-Demand Capacity Reservations

As Reservas de Capacidade sob demanda permitem que você reserve capacidade computacional para suas instâncias do Amazon EC2 por qualquer duração em uma determinada zona de disponibilidade. Permite criar e gerenciar Reservas de Capacidade independentemente dos descontos de faturamento oferecidos por Savings Plans ou Instâncias reservadas regionais.

Ao criar Reservas de Capacidade, você garante sempre ter acesso à capacidade do EC2 quando precisar, por quanto tempo precisar dela. É possível criar Reservas de Capacidade a qualquer momento, sem entrar em um termo de compromisso de um a três anos, e a capacidade fica disponível imediatamente. O faturamento começa assim que a capacidade é provisionada e o(a) Reserva de capacidade entra no estado ativo. Quando você não precisar mais dela, cancele a Reserva de capacidade para não incorrer em cobranças.

Ao criar uma Reserva de capacidade, especifique:

- A zona de disponibilidade na qual reservar a capacidade
- O número de instâncias para as quais reservar capacidade
- Os atributos da instância, incluindo o tipo de instância, a locação e a plataforma ou o sistema operacional

Reservas de Capacidade só podem ser usadas por instâncias que correspondam aos seus atributos. Por padrão, elas são usadas automaticamente por instâncias em execução que correspondem aos atributos. Se você não tiver nenhuma instância em execução que corresponda aos atributos da Reserva de capacidade, ela permanecerá não utilizada até você executar uma instância com atributos correspondentes.

Além disso, é possível usar Savings Plans e instâncias reservadas regionais com Reservas de Capacidade para aproveitar os benefícios dos descontos de faturamento. A AWS aplica automaticamente o desconto quando os atributos de uma reserva de capacidade correspondem aos atributos de um Savings Plan ou de uma instância reservada regional. Para obter mais informações, consulte [Descontos de faturamento \(p. 394\)](#).

Tópicos

- [Diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans \(p. 391\)](#)
- [Plataformas compatíveis \(p. 392\)](#)
- [Limites da Reserva de capacidade \(p. 392\)](#)
- [Restrições e limitações de Reserva de capacidade \(p. 392\)](#)
- [Definição de preços e faturamento da Reserva de capacidade \(p. 393\)](#)
- [Como trabalhar com Reservas de Capacidade \(p. 394\)](#)
- [Reservas de Capacidade em Local Zones \(p. 404\)](#)
- [Reservas de Capacidade em zonas Wavelength \(p. 404\)](#)
- [Reservas de Capacidade no AWS Outposts \(p. 405\)](#)
- [Como trabalhar com Reservas de Capacidade compartilhadas \(p. 406\)](#)
- [Métricas do CloudWatch para Reservas de Capacidade sob demanda \(p. 410\)](#)

Diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans

A tabela a seguir destaca as principais diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans:

	Capacity Reservations	Instâncias reservadas zonais	Instâncias reservadas regionais	Savings Plans
Prazo	Nenhum compromisso é necessário. Podem ser criadas e canceladas conforme necessário.	Exige compromisso fixo de um ano ou de três anos		
Benefício da capacidade	Capacidade reservada em uma zona de disponibilidade específica.		Nenhuma capacidade reservada.	
Desconto de faturamento	Sem desconto de faturamento. †	Fornece um desconto de faturamento.		
Limites de instâncias	Seus limites instância sob demanda por região se aplicam.	O padrão é 20 por zona de disponibilidade. Você	O padrão é 20 por região. Você pode solicitar um aumento de limite.	Sem limite.

	Capacity Reservations	Instâncias reservadas zonais	Instâncias reservadas regionais	Savings Plans
		pode solicitar um aumento de limite.		

† Você pode combinar Reservas de Capacidade com Savings Plans ou instâncias reservadas regionais para receber um desconto.

Para obter mais informações, consulte:

- [Reserved Instances \(p. 259\)](#)
- [Guia do usuário do Savings Plans](#)

Plataformas compatíveis

Você deve criar a reserva de capacidade com a plataforma correta para garantir que ela corresponda corretamente às suas instâncias. As Reservas de Capacidade oferecem suporte às plataformas a seguir:

- Windows
- Windows com SQL Server
- Windows com SQL Server Web
- Windows com SQL Server Standard
- Windows com SQL Server Enterprise

Quando adquire uma Reserva de capacidade, você deve escolher uma oferta para uma plataforma que represente o sistema operacional da sua instância.

- Para Windows com SQL Standard, Windows com SQL Server Enterprise e Windows com SQL Server Web, você deve escolher a plataforma específica.
- Para todas as outras versões do Windows, excluindo BYOL que não é suportado, escolha a plataforma Windows.

Para obter mais informações sobre as plataformas Linux compatíveis, consulte [Plataformas compatíveis](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Limites da Reserva de capacidade

O número de instâncias para as quais você tem permissão para reservar capacidade é baseado no limite de instância sob demanda de sua conta. Você pode reservar capacidade para todas as instâncias permitidas pelo limite, menos o número de instâncias que já estão em execução.

Restrições e limitações de Reserva de capacidade

Antes de criar Reservas de Capacidade, observe as seguintes limitações e restrições.

- Reservas de Capacidade ativas e não utilizadas entram na contagem dos limites de instância sob demanda.
- As Reservas de Capacidade não são transferíveis de uma conta da AWS para outra. No entanto, você pode compartilhar Reservas de Capacidade com outras contas da AWS. Para obter mais informações, consulte [Como trabalhar com Reservas de Capacidade compartilhadas \(p. 406\)](#).
- Os descontos de faturamento Instância reservada de zona não se aplicam às Reservas de Capacidade.

- As Reservas de Capacidade não podem ser criadas em placement groups.
- As Reservas de Capacidade não podem ser usadas com Hosts dedicados.
- As Reservas de Capacidade não podem ser usadas com a política “Traga sua própria licença” (BYOL).
- O Reservas de Capacidade não garante que uma instância hibernada possa retomar depois de tentar iniciá-la.

Definição de preços e faturamento da Reserva de capacidade

O preço de um Reserva de capacidade varia de acordo com a opção de pagamento.

Pricing

Quando o(a) Reserva de capacidade entra no estado `active`, você recebe a cobrança da taxa sob demanda equivalente independentemente de executar instâncias na capacidade reservada ou não. Se você não usar a reserva, ela será exibida como uma reserva não utilizada em sua fatura do EC2. Quando executa uma instância que corresponde aos atributos de uma reserva, você paga apenas pela instância e nada pela reserva. Não há cobranças antecipadas ou adicionais.

Por exemplo, se criar uma Reserva de capacidade para 20 instâncias `m4.large` do Linux e executar 15 instâncias `m4.large` do Linux na mesma zona de disponibilidade, você será cobrado por 15 instâncias ativas e por 5 instâncias não usadas na reserva.

Descontos de faturamento para Savings Plans e Instâncias reservadas regionais aplicam-se a Reservas de Capacidade. Para obter mais informações, consulte [Descontos de faturamento \(p. 394\)](#).

Para obter mais informações, consulte [Definição de preço Amazon EC2](#).

Billing

O faturamento começa assim que a capacidade for provisionada e o(a) Reserva de capacidade entrar no estado `active`. Ele prosseguirá enquanto o(a) Reserva de capacidade permanecer no estado `active`.

As Reservas de Capacidade são cobradas por granularidade por segundo. Isso significa que você é cobrado por horas parciais. Por exemplo, se uma reserva permanecer ativa em sua conta por 24 horas e 15 minutos, você será cobrado por 24,25 horas de reserva.

O exemplo a seguir mostra como uma Reserva de capacidade é cobrada. A Reserva de capacidade é criada para uma instância `m4.large` do Linux, que tem uma taxa sob demanda de 0,10 USD por hora de uso. Neste exemplo, a Reserva de capacidade está ativa na conta por cinco horas. A Reserva de capacidade não é usada na primeira hora, portanto, é cobrada por uma hora não utilizada na taxa sob demanda padrão do tipo de instância `m4.large`. Das duas às cinco horas, a Reserva de capacidade é ocupada por uma instância `m4.large`. Durante esse período, a Reserva de capacidade não acumula cobranças e, em vez disso, a conta é cobrada pela instância `m4.large` que a está ocupando. Na sexta hora, a Reserva de capacidade é cancelada, e a instância `m4.large` é executada normalmente fora da capacidade reservada. Para essa hora, ela é cobrada pela taxa sob demanda do tipo de instância `m4.large`.

Hour	1	2	3	
Unused Capacity Reservation	\$0.10	\$0.00	\$0.00	\$
On-demand Instance Usage	\$0.00	\$0.10	\$0.10	\$
Hourly cost	\$0.10	\$0.10	\$0.10	\$

Descontos de faturamento

Os descontos de faturamento para Savings Plans e instâncias reservadas regionais aplicam-se a Reservas de Capacidade. A AWS aplica automaticamente esses descontos às Reservas de Capacidade que têm atributos correspondentes. Quando uma Reserva de capacidade é usada por uma instância, o desconto é aplicado à instância. Os descontos são preferencialmente aplicados ao uso de instâncias antes de cobrir Reservas de Capacidade não utilizadas.

Os descontos de faturamento de Instâncias reservadas zonais não se aplicam às Reservas de Capacidade.

Para obter mais informações, consulte:

- [Reserved Instances \(p. 259\)](#)
- [Guia do usuário do Savings Plans](#)

Visualizar sua fatura

É possível revisar as cobranças e taxas da sua conta no console do AWS Billing and Cost Management.

- O Painel exibe um resumo de gastos da sua conta.
- Na página Bills (Faturas), em Details (Detalhes), expanda a seção Elastic Compute Cloud e a região para obter informações de faturamento sobre suas Reservas de Capacidade.

Você pode visualizar as cobranças online ou baixar um arquivo CSV. Para obter mais informações, consulte [Itens de linha da reserva de capacidade](#) no Manual do usuário do AWS Billing and Cost Management.

Como trabalhar com Reservas de Capacidade

Para começar a usar as Reservas de Capacidade, crie a reserva de capacidade na zona de disponibilidade exigida. Depois, é possível executar instâncias na capacidade reservada, visualizar a utilização da capacidade em tempo real e aumentar ou diminuir a capacidade conforme necessário.

Por padrão, as Reservas de Capacidade correspondem automaticamente a novas instâncias e instâncias em execução que têm atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade). Isso significa que qualquer instância com atributos correspondentes são automaticamente executadas na Reserva de capacidade. No entanto, você também pode destinar uma Reserva de capacidade para workloads específicas. Isso permite que você controle explicitamente quais instâncias têm permissão para executar na capacidade reservada.

Você pode especificar como a reserva termina. Você pode escolher cancelar o(a) Reserva de capacidade ou encerrá-lo(a) automaticamente em um horário especificado. Se você especificar um horário de término, a Reserva de capacidade será cancelada dentro de uma hora do horário especificado. Por exemplo, se você especificar, 5/31/2019, 13:30:55, a Reserva de capacidade será encerrada entre 13:30:55 e 14:30:55 em 5/31/2019. Após o término da reserva, você não poderá mais destinar instâncias à Reserva de capacidade. Instâncias em execução na capacidade reservada continuam a executar sem interrupção. Se as instâncias que estão destinando uma Reserva de capacidade forem interrompidas, você não poderá reiniciá-las até que a preferência de destino na Reserva de capacidade seja removida ou que você as configure para destinar uma Reserva de capacidade diferente.

Sumário

- [Criar uma Reserva de capacidade \(p. 395\)](#)
- [Trabalhar com grupos de Reserva de capacidade \(p. 396\)](#)
- [Iniciar instâncias em uma Reserva de capacidade existente \(p. 400\)](#)
- [Modifique uma Reserva de capacidade \(p. 401\)](#)

- [Modificar as configurações da Reserva de capacidade de uma instância \(p. 401\)](#)
- [Visualizar uma Reserva de capacidade \(p. 402\)](#)
- [Cancelar uma Reserva de capacidade \(p. 403\)](#)

Criar uma Reserva de capacidade

Depois de criar a Reserva de capacidade, a capacidade estará disponível imediatamente. A capacidade permanece reservada para seu uso enquanto a Reserva de capacidade estiver ativa, e você pode executar instâncias nela a qualquer momento. Se a Reserva de capacidade estiver aberta, as novas instâncias e as instâncias existentes que tiverem atributos correspondentes serão executadas automaticamente na capacidade da Reserva de capacidade. Se a Reserva de capacidade for `targeted`, as instâncias deverão usá-la como destino especificamente para executar na capacidade reservada.

Sua solicitação de criação de uma Reserva de capacidade poderá falhar se uma das seguintes opções for verdadeira:

- O Amazon EC2 não tem capacidade suficiente para realizar a solicitação. Tente novamente mais tarde, tente uma zona de disponibilidade diferente ou tente uma capacidade menor. Se a sua aplicação for flexível entre tipos e tamanhos de instâncias, tente diferentes atributos de instância.
- A quantidade solicitada excede o limite de instância sob demanda para a família de instâncias selecionada. Aumente o limite de instância sob demanda para a família de instâncias e tente novamente. Para obter mais informações, consulte [Limites de instância sob demanda \(p. 256\)](#).

Para criar uma Reserva de capacidade usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione Reservas de Capacidade e Create Reserva de capacidade (Criar Reserva de capacidade).
3. Na página Create a Reserva de capacidade (Criar uma Reserva de capacidade), defina as seguintes configurações na seção Instance details (Detalhes da instância): O tipo de instância, a plataforma e a zona de disponibilidade das instâncias iniciadas devem corresponder ao tipo de instância, à plataforma e à zona de disponibilidade especificadas aqui ou a Reserva de capacidade não será aplicada. Por exemplo, se uma Reserva de capacidade aberta não corresponder, a execução de uma instância que for destinada a essa Reserva de capacidade explicitamente falhará.
 - a. Instance Type (Tipo de instância) — o tipo de instância a ser executada na capacidade reservada.
 - b. Launch EBS-optimized instances (Executar instâncias otimizadas para EBS) — especifique se deseja reservar a capacidade para instâncias otimizadas para EBS. Essa opção é selecionada por padrão para alguns tipos de instância. Para obter mais informações sobre instâncias otimizadas para EBS, consulte [Amazon Elastic Block Store \(p. 1243\)](#).
 - c. Attach instance store at launch (Anexar armazenamento de instâncias na execução) — especifique se as instâncias executadas na Reserva de capacidade usam armazenamento temporário em nível de bloco. Os dados em um volume de armazenamento de instâncias persistem apenas durante a vida útil da instância associada.
 - d. Platform (Plataforma) — o sistema operacional das suas instâncias. Para obter mais informações, consulte [Plataformas compatíveis \(p. 392\)](#). Para obter mais informações sobre as plataformas Linux compatíveis, consulte [Plataformas compatíveis](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.
 - e. Availability Zone (Zona de disponibilidade) — a zona de disponibilidade na qual reservar a capacidade.
 - f. Tenancy (Locação) — especifique se você quer executar em hardware compartilhado (padrão) ou em uma instância dedicada.
 - g. Quantity (Quantidade) — o número de instâncias para as quais reservar a capacidade. Se você especificar uma quantidade que exceda seu limite de instância sob demanda restante para o tipo de instância selecionado, a solicitação será negada.

4. Defina as seguintes configurações na seção Reservation details (Detalhes da reserva):
 - a. Reservation Ends (Término da reserva) — escolha somente uma das duas opções a seguir:
 - Manually (Manualmente) — reserve a capacidade até que você a cancele explicitamente.
 - Specific time (Horário específico) — cancele a reserva de capacidade automaticamente na data e na hora especificadas.
 - b. Instance eligibility (Qualificação de instância) — escolha uma das seguintes opções:
 - open (aberta) — (padrão) a Reserva de capacidade corresponde a qualquer instância que tenha atributos correspondentes (tipo, plataforma e zona de disponibilidade da instância). Se você executar uma instância com atributos correspondentes, ela será colocada na capacidade reservada automaticamente.
 - targeted (destinada) — a Reserva de capacidade só aceita instâncias que tenham atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade) e estejam explicitamente destinadas para a reserva.
5. Escolha Request reservation (Solicitar reserva).

Para criar uma reserva de capacidade usando a AWS CLI

Use o comando [create-capacity-reservation](#). Para obter mais informações, consulte [Plataformas compatíveis \(p. 392\)](#). Para obter mais informações sobre as plataformas Linux compatíveis, consulte [Plataformas compatíveis](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Por exemplo, o comando a seguir cria uma Reserva de capacidade que reserva capacidade para três instâncias m5.2xlarge, executando o Windows com AMIs do SQL Server na zona de disponibilidade us-east-1a.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-platform Windows  
with SQL Server --availability-zone us-east-1a --instance-count 3
```

Trabalhar com grupos de Reserva de capacidade

Você pode usar o AWS Resource Groups para criar coleções lógicas de Reservas de Capacidade, chamadas grupos de recursos. Um grupo de recursos é um agrupamento lógico de recursos da AWS que estão todos na mesma região da AWS. Você pode incluir várias Reservas de Capacidade com atributos diferentes (tipo de instância, plataforma e zona de disponibilidade) em um único grupo de recursos.

Ao criar grupos de recursos para Reservas de Capacidade, você pode direcionar instâncias a um grupo de Reservas de Capacidade, em vez de uma Reserva de capacidade individual. As instâncias direcionadas a um grupo de Reservas de Capacidade estabelecem correspondência com qualquer Reserva de capacidade do grupo que tenha atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade) e capacidade disponível. Se o grupo não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas usando a capacidade sob demanda. Se uma Reserva de capacidade correspondente for adicionada ao grupo de destino em um estágio posterior, a correspondência da instância será automática e ela será movida para sua capacidade reservada.

Para evitar o uso não intencional de Reservas de Capacidade em um grupo, configure as Reservas de Capacidade no grupo para aceitar somente as instâncias que se dirigem explicitamente à reserva de capacidade. Para fazer isso, defina Instance eligibility (Qualificação de instâncias) como targeted (direcionadas) ou Only instances that specify this reservation (Somente instâncias que especificam essa reserva) (novo console) ao criar a Reserva de capacidade usando o console do Amazon EC2. Ao usar a AWS CLI, especifique `--instance-match-criteria targeted` ao criar a reserva de capacidade. Isso garante que somente as instâncias explicitamente direcionadas ao grupo, ou a uma Reserva de capacidade no grupo, possam ser executadas no grupo.

Se uma Reserva de capacidade em um grupo for cancelada ou expirar enquanto tiver instâncias em execução, as instâncias serão automaticamente movidas para outra Reserva de capacidade no grupo que tenha atributos correspondentes e capacidade disponível. Se não houver Reservas de Capacidade restantes no grupo que tenham atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda. Se uma Reserva de capacidade correspondente for adicionada ao grupo de destino em um estágio posterior, a instância será automaticamente movida para sua capacidade reservada.

Como criar um grupo para Reservas de Capacidade

Use o comando [create-group](#) da AWS CLI. Para `name`, forneça um nome descritivo para o grupo e, para `configuration`, especifique dois parâmetros de solicitação `Type`:

- `AWS::EC2::CapacityReservationPool` para garantir que o grupo de recursos possa ser direcionado para execuções de instâncias
- `AWS::ResourceGroups::Generic` com `allowed-resource-types` definido como `AWS::EC2::CapacityReservation` para garantir que o grupo de recursos aceite apenas Reservas de Capacidade

Por exemplo, o comando a seguir cria um grupo chamado `MyCRGroup`.

```
C:\> aws resource-groups create-group --name MyCRGroup --configuration
'{"Type":"AWS::EC2::CapacityReservationPool"}' '{"Type":"AWS::ResourceGroups::Generic",
"Parameters": [{"Name": "allowed-resource-types", "Values":
["AWS::EC2::CapacityReservation"]}]}'
```

Veja a seguir um exemplo de saída.

```
{
    "GroupConfiguration": {
        "Status": "UPDATE_COMPLETE",
        "Configuration": [
            {
                "Type": "AWS::EC2::CapacityReservationPool"
            },
            {
                "Type": "AWS::ResourceGroups::Generic",
                "Parameters": [
                    {
                        "Values": [
                            "AWS::EC2::CapacityReservation"
                        ],
                        "Name": "allowed-resource-types"
                    }
                ]
            }
        ],
        "Group": {
            "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
            "Name": "MyCRGroup"
        }
    }
}
```

Como adicionar uma Reserva de capacidade a um grupo

Use o comando [group-resources](#) da AWS CLI. Para `group`, especifique o nome do grupo ao qual adicionar as Reservas de Capacidade e, para `resources`, especifique ARNs de Reservas de Capacidade a serem adicionadas. Para adicionar várias Reservas de Capacidade, separe os ARNs com um espaço. Para obter

os ARNs das Reservas de Capacidade para adicionar, use o comando [describe-capacity-reservations](#) da AWS CLI e especifique os IDs das Reservas de Capacidade.

Por exemplo, o comando a seguir adiciona duas Reservas de Capacidade a um grupo chamado MyCRGroup.

```
C:\> aws resource-groups group-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Veja a seguir um exemplo de saída.

```
{  
    "Failed": [],  
    "Succeeded": [  
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",  
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"  
    ]  
}
```

Como visualizar as Reservas de Capacidade em um grupo específico

Use o comando [list-group-resources](#) da AWS CLI. Para group, especifique o nome do grupo.

Por exemplo, o comando a seguir lista as Reservas de Capacidade em um grupo chamado MyCRGroup.

```
C:\> aws resource-groups list-group-resources --group MyCRGroup
```

Veja a seguir um exemplo de saída.

```
{  
    "QueryErrors": [],  
    "ResourceIdentifiers": [  
        {  
            "ResourceType": "AWS::EC2::CapacityReservation",  
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1"  
        },  
        {  
            "ResourceType": "AWS::EC2::CapacityReservation",  
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"  
        }  
    ]  
}
```

Como exibir os grupos aos quais uma reserva de capacidade específica foi adicionada (AWS CLI)

Use o comando [get-groups-for-capacity-reservation](#) da AWS CLI.

Por exemplo, o comando a seguir lista os grupos aos quais a Reserva de capacidade cr-1234567890abcdef1 foi adicionada.

```
C:\> aws ec2 get-groups-for-capacity-reservation --capacity-reservation-id cr-1234567890abcdef1
```

Veja a seguir um exemplo de saída.

```
{  
    "CapacityReservationGroups": [  
        {  
            "OwnerId": "123456789012",  
            "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup"  
        }  
    ]  
}
```

Como visualizar os grupos aos quais uma Reserva de capacidade específica foi adicionada (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reservas de Capacidade, selecione a Reserva de capacidade a ser visualizada e escolha View (Visualizar).

Os grupos aos quais a Reserva de capacidade foi adicionada são listados no cartão Groups (Grupos).

Como remover uma Reserva de capacidade de um grupo

Use o comando [ungroup-resources](#) da AWS CLI. Para group, especifique o ARN do grupo do qual remover a Reserva de capacidade e, para resources, especifique os ARNs das Reservas de Capacidade a serem removidas. Para remover várias Reservas de Capacidade, separe os ARNs com um espaço.

O exemplo a seguir remove duas Reservas de Capacidade de um grupo chamado MyCRGroup.

```
C:\> aws resource-groups ungroup-resources --group MyCRGroup --  
resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/  
cr-0e154d26a16094dd arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/  
cr-54321abcdef567890
```

Veja a seguir um exemplo de saída.

```
{  
    "Failed": [],  
    "Succeeded": [  
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd",  
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"  
    ]  
}
```

Para excluir um grupo

Use o comando [delete-group](#) da AWS CLI. Para group, forneça o nome do grupo a ser excluído.

Por exemplo, o comando a seguir exclui um grupo chamado MyCRGroup.

```
C:\> aws resource-groups delete-group --group MyCRGroup
```

Veja a seguir um exemplo de saída.

```
{  
    "Group": {  
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",  
        "Name": "MyCRGroup"  
    }  
}
```

}

Iniciar instâncias em uma Reserva de capacidade existente

Ao executar uma instância, você pode especificar se deseja executá-la em qualquer Reserva de capacidade open, em uma Reserva de capacidade específica ou em um grupo de Reservas de Capacidade. Você só pode executar uma instância em uma Reserva de capacidade que tenha atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade) e capacidade suficiente. Se preferir, configure a instância para evitar a execução em um Reserva de capacidade, mesmo que você tenha uma Reserva de capacidade open com atributos correspondentes e capacidade disponível.

A execução de uma instância em uma Reserva de capacidade reduz a capacidade disponível pelo número de instâncias executadas. Por exemplo, se você executar três instâncias, a capacidade disponível da Reserva de capacidade será reduzida em três.

Para executar instâncias em uma Reserva de capacidade existente usando o console

1. Abra o assistente de execução de instâncias selecionando Launch Instances (Executar instâncias) em Dashboard (Painel) ou Instances (Instâncias).
2. Selecione uma imagem de máquina da Amazon (AMI) e um tipo de instância.
3. Conclua a página Configure Instance Details (Configurar detalhes da instância). Para Reserva de capacidade, selecione uma das seguintes opções:
 - None (Nenhuma) — impede que as instâncias sejam executadas em uma Reserva de capacidade. As instâncias são executadas na capacidade sob demanda.
 - Open (Aberta) — executa as instâncias em qualquer Reserva de capacidade que tenha atributos correspondentes e capacidade suficiente para o número de instâncias selecionadas. Se você não tiver uma Reserva de capacidade correspondente com capacidade suficiente, a instância usará a capacidade sob demanda.
 - Target by ID (Alvo por ID) — executa as instâncias na Reserva de capacidade selecionada. Se a Reserva de capacidade selecionada não tiver capacidade suficiente para o número de instâncias selecionadas, a execução da instância falhará.
 - Target by group (Alvo por grupo) — executa as instâncias em qualquer Reserva de capacidade com atributos correspondentes e capacidade disponível no grupo de Reserva de capacidade selecionado. Se o grupo selecionado não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda.
4. Conclua as etapas restantes para executar as instâncias.

Para executar uma instância em uma Reserva de capacidade existente usando a AWS CLI

Use o comando `run-instances` e especifique o parâmetro `--capacity-reservation-specification`.

O exemplo a seguir executa uma instância `t2.micro` em qualquer Reserva de capacidade aberta que tenha atributos correspondentes e capacidade disponível:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-specification CapacityReservationPreference=open
```

O exemplo a seguir executa uma instância `t2.micro` em uma Reserva de capacidade `targeted`:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-specification CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

O exemplo a seguir executa uma instância t2.micro em um grupo de Reserva de capacidade:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-specification CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-groups:us-west-1:123456789012:group/my-cr-group}
```

Modifique uma Reserva de capacidade

É possível alterar os atributos de uma Reserva de capacidade ativa depois de criá-la. Não é possível modificar uma Reserva de capacidade depois que ela expirar ou depois de você cancelá-la explicitamente.

Ao modificar uma Reserva de capacidade, você só pode aumentar ou diminuir a quantidade e alterar a maneira como ela é lançada. Não é possível alterar o tipo de instância, a otimização de EBS, as configurações de armazenamento de instâncias, a plataforma, a zona de disponibilidade nem a qualificação de instâncias de uma Reserva de capacidade. Se for necessário modificar qualquer um desses atributos, recomendamos cancelar a reserva e, em seguida, criar uma nova com os atributos necessários.

Se você especificar uma nova quantidade que exceda seu limite de instância sob demanda restante para o tipo de instância selecionada, a atualização falhará.

Para modificar uma Reserva de capacidade usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Reservas de Capacidade, selecione a Reserva de capacidade a ser modificada e, em seguida, escolha Edit (Editar).
3. Modifique as opções Quantity (Quantidade) ou Reservation ends (Término da reserva) conforme necessário e escolha Save changes (Salvar alterações).

Para modificar uma reserva de capacidade usando a AWS CLI

Use o comando [modify-capacity-reservations](#):

Por exemplo, o comando a seguir modifica uma Reserva de capacidade para reservar capacidade para oito instâncias.

```
aws ec2 modify-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0 --instance-count 8
```

Modificar as configurações da Reserva de capacidade de uma instância

É possível modificar as configurações da Reserva de capacidade a seguir para uma instância interrompida a qualquer momento:

- Comece em qualquer Reserva de capacidade que tenha atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade) e capacidade disponível.
- Execute a instância em uma Reserva de capacidade específica.
- Inicie a instância em qualquer Reserva de capacidade que tenha atributos correspondentes e capacidade disponível em um grupo de Reserva de capacidade
- Impeda que a instância seja iniciada em uma Reserva de capacidade.

Para modificar as configurações da Reserva de capacidade de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. Escolha Instances (Instâncias) e selecione a instância a ser modificada. Interrompa a instância se ela ainda não tiver sido interrompida.
3. Escolha Actions (Ações), Modify Reserva de capacidade Settings (Modificar configurações da Reserva de capacidade).
4. Para Reserva de capacidade, selecione uma das seguintes opções:
 - Open (Aberta) — executa as instâncias em qualquer Reserva de capacidade que tenha atributos correspondentes e capacidade suficiente para o número de instâncias selecionadas. Se você não tiver uma Reserva de capacidade correspondente com capacidade suficiente, a instância usará a capacidade sob demanda.
 - None (Nenhuma) — impede que as instâncias sejam executadas em uma Reserva de capacidade. As instâncias são executadas na capacidade sob demanda.
 - Specify Capacity Reservation (Especificar reserva de capacidade) — executa as instâncias na Reserva de capacidade selecionada. Se a Reserva de capacidade selecionada não tiver capacidade suficiente para o número de instâncias selecionadas, a execução da instância falhará.
 - Specify Capacity Reservation group (Especificar grupo de reserva de capacidade) — executa as instâncias em qualquer Reserva de capacidade com atributos correspondentes e capacidade disponível no grupo de Reserva de capacidade selecionado. Se o grupo selecionado não tiver uma Reserva de capacidade com atributos correspondentes e capacidade disponível, as instâncias serão executadas na capacidade sob demanda.

Para modificar as configurações da reserva de capacidade de uma instância usando a AWS CLI

Use o comando [modify-instance-capacity-reservation-attributes](#).

Por exemplo, o comando a seguir altera a configuração da Reserva de capacidade de uma instância para open ou none.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-id i-1234567890abcdef0  
--capacity-reservation-specification CapacityReservationPreference=none|open
```

Por exemplo, o comando a seguir modifica uma instância para ter como destino uma Reserva de capacidade específica.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-  
id i-1234567890abcdef0 --capacity-reservation-specification  
CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

Por exemplo, o comando a seguir modifica uma instância para ter como destino um grupo de Reserva de capacidade específico.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-  
id i-1234567890abcdef0 --capacity-reservation-specification  
CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-groups:us-  
west-1:123456789012:group/my-cr-group}
```

Visualizar uma Reserva de capacidade

As Reservas de Capacidade têm estes estados possíveis:

- active — a capacidade está disponível para uso.
- expired — a Reserva de capacidade expirou automaticamente na data e hora especificadas em sua solicitação de reserva. A capacidade reservada não está mais disponível para uso.
- cancelled—O(A) Reserva de capacidade foi cancelado(a). A capacidade reservada não está mais disponível para uso.

- **pending** — a solicitação de Reserva de capacidade foi bem-sucedida, mas o provisionamento da capacidade ainda está pendente.
- **failed** — a solicitação da Reserva de capacidade falhou. Uma solicitação pode falhar devido a parâmetros de solicitação inválidos, restrições da capacidade ou restrições de limite de instâncias. É possível visualizar uma solicitação com falha por 60 minutos.

Para visualizar as Reservas de Capacidade usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Reservas de Capacidade e selecione uma Reserva de capacidade para visualizar.
3. Escolha View launched instances for this reservation (Visualizar instâncias executadas para essa reserva)

Para visualizar as Reservas de Capacidade usando a AWS CLI

Use o comando [describe-capacity-reservations](#):

Por exemplo, o comando a seguir descreve todas as Reservas de Capacidade.

```
aws ec2 describe-capacity-reservations
```

Cancelar uma Reserva de capacidade

Você pode cancelar uma Reserva de capacidade a qualquer momento se não precisar mais da capacidade reservada. Quando você cancela uma Reserva de capacidade, a capacidade é liberada imediatamente e não é mais reservada para seu uso.

Você pode cancelar Reservas de Capacidade vazias e Reservas de Capacidade que têm instâncias em execução. Se você cancelar uma Reserva de capacidade que tenha instâncias em execução, as instâncias continuarão a ser executadas normalmente fora da reserva da capacidade em taxas padrão de instância sob demanda ou em uma tarifa com desconto, se você tiver um Savings Plan ou uma Instância reservada regional correspondente.

Depois que você cancela uma Reserva de capacidade, as instâncias que a usavam como destino não podem mais ser executadas. Modifique essas instâncias para que elas tenham outra Reserva de capacidade como destino, sejam executadas em uma Reserva de capacidade aberta com atributos correspondentes e capacidade suficiente ou evitem a execução em uma Reserva de capacidade. Para obter mais informações, consulte [Modificar as configurações da Reserva de capacidade de uma instância](#) (p. 401).

Para cancelar uma Reserva de capacidade usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Reservas de Capacidade e selecione a Reserva de capacidade a ser cancelada.
3. Escolha Cancel reservation (Cancelar reserva), Cancel reservation (Cancelar reserva).

Para cancelar uma reserva de capacidade usando a AWS CLI

Use o comando [cancel-capacity-reservation](#):

Por exemplo, o comando a seguir cancela uma Reserva de capacidade com um ID `cr-1234567890abcdef0`.

```
aws ec2 cancel-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0
```

Reservas de Capacidade em Local Zones

Uma Local Zone é uma extensão de uma região da AWS que está geograficamente próxima de seus usuários. Os recursos criados em uma Local Zone podem atender usuários locais com comunicações de latência muito baixa. Para obter mais informações, consulte [Local ZonesAWS](#).

É possível estender uma VPC de sua região da AWS pai para uma Local Zone criando uma sub-rede nessa Local Zone. Quando você criar uma sub-rede em uma Local Zone, sua VPC também será estendida para essa Local Zone. A sub-rede na Local Zone funciona da mesma forma que outras sub-redes na VPC.

Ao usar Local Zones, é possível colocar Reservas de Capacidade em vários locais que estão mais próximos de seus usuários. Você cria e usa Reservas de Capacidade em Local Zones da mesma forma que cria e usa Reservas de Capacidade em zonas de disponibilidade regulares. Os mesmos recursos e comportamento de correspondência de instâncias são aplicados. Para obter mais informações sobre os modelos de preço com suporte nas Local Zones, consulte [AWS Local Zones FAQs \(Perguntas frequentes sobre AWS Local Zones\)](#).

Considerations

Não é possível usar grupos de Reserva de capacidade em uma Local Zone.

Para usar uma reserva de capacidade em uma Local Zone

1. Habilite a Local Zone para usar em sua conta da AWS. Para obter mais informações, consulte [Habilitar Local Zones](#) no Manual do usuário do Amazon EC2 para instâncias do Linux.
2. Crie uma reserva de capacidade na Local Zone. Para Availability Zone (Zona de disponibilidade), escolha a Local Zone. A Local Zone é representada por um código de região da AWS seguido por um identificador que indica o local, por exemplo, us-west-2-lax-1a. Para obter mais informações, consulte [Criar uma Reserva de capacidade \(p. 395\)](#).
3. Crie uma sub-rede na Local Zone. Para Availability Zone (Zona de disponibilidade), escolha a Local Zone. Para obter mais informações, consulte [Criar uma sub-rede na VPC](#) no Guia do usuário da Amazon VPC.
4. Execute uma instância. Em Subnet (Sub-rede), escolha a sub-rede na Local Zone (por exemplo `subnet-123abc | us-west-2-lax-1a`) e em Capacity Reservation (Reserva de capacidade), escolha a especificação (open ou indique seu ID) necessária para a reserva de capacidade que você criou na Local Zone. Para obter mais informações, consulte [Iniciar instâncias em uma Reserva de capacidade existente \(p. 400\)](#).

Reservas de Capacidade em zonas Wavelength

O AWS Wavelength permite que os desenvolvedores criem aplicações que oferecem baixíssimas latências para dispositivos móveis e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação. Você pode estender uma Amazon Virtual Private Cloud (VPC) para uma ou mais zonas de Wavelength. Em seguida, você pode usar recursos da AWS como instâncias do Amazon EC2 para executar aplicações que exigem latência ultrabaixa e uma conexão com produtos da AWS na região. Para obter mais informações, consulte [AWS Wavelength Zonas](#).

Ao criar Reservas de Capacidade sob demanda, você pode escolher a zona de Wavelength e executar instâncias de Reserva de capacidade em uma zona de Wavelength especificando a sub-rede associada à zona de Wavelength. Uma zona do Wavelength é representada por um código de região da AWS seguido por um identificador que indica o local, por exemplo, us-east-1-wl1-bos-wlz-1.

As zonas de Wavelength não estão disponíveis em todas as regiões. Para obter informações sobre as regiões compatíveis com as zonas do Wavelength consulte [Zonas do Wavelength disponíveis](#) no Guia do desenvolvedor da AWS Wavelength.

Considerations

Não é possível usar grupos de Reserva de capacidade em uma zona de Wavelength.

Para usar uma Reserva de capacidade em uma zona de Wavelength

1. Habilite a zona do Wavelength para uso em sua conta da AWS. Para obter mais informações, consulte [Ativar zonas de Wavelength](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.
2. Crie uma Reserva de capacidade na zona de Wavelength. Para Availability Zone (Zona de disponibilidade), escolha a Wavelength. O Wavelength é representado por um código de região da AWS seguido por um identificador que indica o local, por exemplo us-east-1-wl1-bos-wlz-1. Para obter mais informações, consulte [Criar uma Reserva de capacidade \(p. 395\)](#).
3. Depois, crie uma sub-rede na zona de Wavelength. Para Availability Zone (Zona de disponibilidade), escolha a zona de Wavelength. Para obter mais informações, consulte [Criar uma sub-rede na VPC](#) no Guia do usuário da Amazon VPC.
4. Execute uma instância. Em Subnet (Sub-rede), escolha a sub-rede na Wavelength (por exemplo subnet-123abc | us-east-1-wl1-bos-wlz-1) e em Reserva de capacidade, escolha a especificação (open ou indique seu ID) necessária para a Reserva de capacidade que você criou na Wavelength. Para obter mais informações, consulte [Iniciar instâncias em uma Reserva de capacidade existente \(p. 400\)](#).

Reservas de Capacidade no AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS no local do cliente. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que os clientes criem e executem aplicações on-premises usando as mesmas interfaces de programação que nas regiões da AWS, ao mesmo tempo que usam recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS.

Você pode criar Reservas de Capacidade nos Outposts que criou na sua conta. Isso permite que você reserve capacidade computacional em um Outpost em seu local. Você cria e usa Reservas de Capacidade em Outposts da mesma forma que cria e usa Reservas de Capacidade em zonas de disponibilidade regulares. Os mesmos recursos e comportamento de correspondência de instâncias são aplicados.

Você também pode compartilhar Reservas de Capacidade em Outposts com outros contas da AWS dentro da organização usando o AWS Resource Access Manager. Para obter mais informações sobre o compartilhamento de Reservas de Capacidade, consulte [Como trabalhar com Reservas de Capacidade compartilhadas \(p. 406\)](#).

Prerequisite

Você deve ter um Outpost instalado em seu local. Para obter mais informações, consulte [Criar um Outpost e solicitar capacidade do Outpost](#) no Manual do usuário do AWS Outposts.

Considerações

- Não é possível usar grupos de reserva de capacidade em um Outpost.

Para usar um grupo de reserva de capacidade em um Outpost

1. Crie uma sub-rede no Outpost. Para obter mais informações, consulte [Criar uma sub-rede no Manual do usuário do AWS Outposts](#).
2. Crie uma reserva de capacidade no Outpost.

- a. Abra o console do AWS Outposts em <https://console.aws.amazon.com/outposts/>.
- b. No painel de navegação, selecione Outposts e, em seguida, escolha Actions (Ações), Create Capacity Reservation (Criar reserva de capacidade).
- c. Configure a reserva de capacidade conforme necessário e escolha Create (Criar). Para obter mais informações, consulte [Criar uma Reserva de capacidade \(p. 395\)](#).

Note

O menu suspenso Instance Type (Tipo de instância) lista somente os tipos de instância que são compatíveis com o Outpost selecionado, e o menu suspenso Availability Zone (Zona de disponibilidade) lista somente a zona de disponibilidade à qual o Outpost selecionado está associado.

3. Iniciar uma instância na reserva de capacidade Em Subnet (Sub-rede), escolha a sub-rede criada na Etapa 1 e, em Capacity Reservation (Reserva de capacidade), selecione a reserva de capacidade criada na Etapa 2. Para obter mais informações, consulte [Executar uma instância no Outpost](#) no Manual do usuário do AWS Outposts.

Como trabalhar com Reservas de Capacidade compartilhadas

O compartilhamento de reserva de capacidade permite que os proprietários de reservas de capacidade compartilhem sua capacidade reservada com outras contas da AWS em uma organização da AWS. Isso permite criar e gerenciar as Reservas de Capacidade centralmente e compartilhar a capacidade reservada entre várias contas da AWS ou em sua organização da AWS.

Nesse modelo, a conta da AWS que possui a Reserva de capacidade (proprietária) compartilha-a com outras contas da AWS (consumidores). Os consumidores podem executar instâncias nas Reservas de Capacidade que são compartilhadas com eles da mesma maneira que executam instâncias em Reservas de Capacidade que possuem em sua própria conta. O proprietário da Reserva de capacidade é responsável pelo gerenciamento da Reserva de capacidade e pelas instâncias que executa nela. Os proprietários não podem modificar as instâncias que os consumidores executam nas Reservas de Capacidade que compartilham. Os consumidores são responsáveis por gerenciar as instâncias que executam em Reservas de Capacidade compartilhadas com eles. Os consumidores não podem visualizar ou modificar instâncias de propriedade de outros consumidores ou do proprietário da Reserva de capacidade.

O proprietário de uma Reserva de capacidade pode compartilhar uma Reserva de capacidade com:

- Contas específicas da AWS dentro ou fora de sua organização na AWS
- Uma unidade organizacional dentro de sua organização da AWS
- Toda a sua organização da AWS

Tópicos

- [Pré-requisitos para compartilhar Reservas de Capacidade \(p. 407\)](#)
- [Serviços relacionados \(p. 407\)](#)
- [Compartilhamento entre zonas de disponibilidade \(p. 407\)](#)
- [Compartilhar uma Reserva de capacidade \(p. 407\)](#)
- [Parar de compartilhar uma Reserva de capacidade \(p. 408\)](#)
- [Identificar uma Reserva de capacidade compartilhada \(p. 409\)](#)
- [Exibir uso de Reserva de capacidade compartilhado \(p. 409\)](#)
- [Permissões de Reserva de capacidade compartilhada \(p. 410\)](#)
- [Faturamento e medição \(p. 410\)](#)

- Limites de instâncias (p. 410)

Pré-requisitos para compartilhar Reservas de Capacidade

- Para compartilhar uma Reserva de capacidade, é necessário ser o proprietário dela em sua conta da AWS. Não é possível compartilhar uma Reserva de capacidade que tenha sido compartilhada com você.
- Só é possível compartilhar Reservas de Capacidade para instâncias de locação compartilhada. Não é possível compartilhar Reservas de Capacidade para instâncias de locação dedicada.
- O compartilhamento de Reserva de capacidade não está disponível para contas novas da AWS ou para contas da AWS que tenham um histórico limitado de faturamento.
- Para compartilhar uma reserva de capacidade com a sua organização da AWS ou com uma unidade organizacional de sua organização da AWS, é necessário habilitar o compartilhamento com o AWS Organizations. Para obter mais informações, consulte [Enable Sharing with AWS Organizations \(Habilitar o compartilhamento com o AWS Organizations\)](#) no AWS RAM User Guide (Manual do usuário do AWS RAM).

Serviços relacionados

O compartilhamento de reserva de capacidade integra-se ao AWS Resource Access Manager (AWS RAM). O AWS RAM é um serviço que permite compartilhar seus recursos da AWS com qualquer conta da AWS ou por meio do AWS Organizations. Com o AWS RAM, você compartilha recursos que possui criando um compartilhamento de recursos. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Os consumidores podem ser contas individuais da AWS, unidades organizacionais ou toda uma organização do AWS Organizations.

Para obter mais informações sobre o AWS RAM, consulte o [Manual do usuário do AWS RAM](#).

Compartilhamento entre zonas de disponibilidade

Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta. Isso pode resultar em diferenças na nomenclatura de zonas de disponibilidade entre contas. Por exemplo, a zona de disponibilidade `us-east-1a` de sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para identificar o local de suas Reservas de Capacidade relativo a suas contas, use o ID da zona de disponibilidade (ID da AZ). O ID da AZ é um identificador exclusivo e consistente de uma zona de disponibilidade em todas as contas da AWS. Por exemplo, `use1-az1` é um ID de AZ da região `us-east-1` e é o mesmo local em cada conta da AWS.

Para visualizar os IDs de AZs das zonas de disponibilidade em sua conta

1. Abra o console do AWS RAM em <https://console.aws.amazon.com/ram>.
2. Os IDs de AZs da região atual são exibidos no painel Your AZ ID (Seu ID de AZ) no lado direito da tela.

Compartilhar uma Reserva de capacidade

Ao compartilhar uma reserva de capacidade de sua propriedade com outras contas da AWS, você permite que elas executem instâncias em sua capacidade reservada. Se você compartilhar uma Reserva de capacidade aberta, lembre-se do seguinte, pois isso pode resultar em uso não intencional da Reserva de capacidade:

- Se os consumidores tiverem instâncias em execução que correspondam aos atributos da Reserva de capacidade, tenham o parâmetro `CapacityReservationPreference` definido como `open` e

ainda não estejam em execução na capacidade reservada, eles usarão a Reserva de capacidade compartilhada automaticamente.

- Se os consumidores executarem instâncias que tenham atributos correspondentes (tipo de instância, plataforma e zona de disponibilidade) e tiverem definido o parâmetro `CapacityReservationPreference` como `open`, eles executarão automaticamente na Reserva de capacidade compartilhada.

Para compartilhar uma Reserva de capacidade, é necessário adicioná-la a um compartilhamento de recursos. Um compartilhamento de recursos é um recurso do AWS RAM que permite que você compartilhe seus recursos entre contas da AWS. Um compartilhamento de recursos especifica os recursos a serem compartilhados, e os consumidores com os quais compartilhá-los. Ao compartilhar uma Reserva de capacidade usando o console do Amazon EC2, você a adiciona a um compartilhamento de recursos existente. Para adicionar a reserva de capacidade a um novo compartilhamento de recursos, você deve criar o compartilhamento de recursos usando o [console do AWS RAM](#).

Se você fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na organização, os consumidores da organização receberão acesso automaticamente à reserva de capacidade compartilhada. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e acesso à Reserva de capacidade compartilhada depois de aceitar o convite.

É possível compartilhar uma reserva de capacidade de sua propriedade usando o console do Amazon EC2, o console do AWS RAM ou a AWS CLI.

Para compartilhar uma Reserva de capacidade de sua propriedade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Escolha a Reserva de capacidade a ser compartilhada e escolha Actions (Ações), Share reservation (Compartilhar reserva).
4. Selecione o compartilhamento de recursos ao qual adicionar a Reserva de capacidade e escolha Share Reserva de capacidade (Compartilhar Reserva de capacidade).

Pode levar alguns minutos para que os consumidores obtenham acesso à Reserva de capacidade compartilhada.

Para compartilhar uma reserva de capacidade de sua propriedade usando o console do AWS RAM

Consulte [Criar um compartilhamento de recursos](#) no Manual do usuário do AWS RAM.

Para compartilhar uma reserva de capacidade de sua propriedade usando a AWS CLI

Use o comando [create-resource-share](#).

Parar de compartilhar uma Reserva de capacidade

O proprietário da Reserva de capacidade pode parar de compartilhar a Reserva de capacidade a qualquer momento. As seguintes regras se aplicam:

- As instâncias de propriedade de consumidores que estavam em execução na capacidade compartilhada na hora do cancelamento do compartilhamento continuam sendo executadas normalmente fora da capacidade reservada, e a capacidade é restaurada para a Reserva de capacidade sujeita à disponibilidade da capacidade do Amazon EC2.
- Os consumidores com quem a Reserva de capacidade era compartilhada não podem mais executar novas instâncias na capacidade reservada.

Para interromper o compartilhamento de uma Reserva de capacidade que você possui, remova-a do compartilhamento de recursos. Isso pode ser feito usando o console do Amazon EC2, o console do AWS RAM ou a AWS CLI.

Como interromper o compartilhamento de uma Reserva de capacidade que você possui usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Selecione a Reserva de capacidade e escolha a guia Sharing (Compartilhamento).
4. A guia Sharing (Compartilhamento) lista os compartilhamentos de recursos aos quais a Reserva de capacidade foi adicionada. Selecione o compartilhamento de recursos do qual remover a Reserva de capacidade e escolha Remove from resource share (Remover do compartilhamento de recursos).

Como interromper o compartilhamento de uma reserva de capacidade que você possui usando o console do AWS RAM

Consulte [Updating a Resource Share \(Atualização de um compartilhamento de recursos\)](#) no AWS RAM User Guide (Manual do usuário do AWS RAM).

Para interromper o compartilhamento de uma reserva de capacidade que você possui usando o console do AWS CLI

Use o comando [disassociate-resource-share](#).

Identificar uma Reserva de capacidade compartilhada

Os proprietários e consumidores podem identificar Reservas de Capacidade compartilhadas usando o console do Amazon EC2 e a AWS CLI

Para identificar uma Reserva de capacidade compartilhada usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reservas de Capacidade. A tela lista as Reservas de Capacidade de sua propriedade e as Reservas de Capacidade que são compartilhadas com você. A coluna Owner (Proprietário) mostra o ID da conta da AWS do proprietário da Reserva de capacidade. O (me) ao lado do ID da conta da AWS indica que você é o proprietário.

Para identificar uma Reserva de capacidade compartilhada usando a AWS CLI

Use o comando [describe-capacity-reservations](#). O comando retorna as Reservas de Capacidade de sua propriedade e as Reservas de Capacidade que são compartilhadas com você. O OwnerId mostra o ID da conta da AWS do proprietário da Reserva de capacidade.

Exibir uso de Reserva de capacidade compartilhado

O proprietário de uma Reserva de capacidade compartilhada pode visualizar seu uso a qualquer momento usando o console do Amazon EC2 e a AWS CLI.

Para visualizar o uso da Reserva de capacidade usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Reservas de Capacidade.
3. Selecione a Reserva de capacidade da qual visualizar o uso e escolha a guia Usage (Uso).

A coluna AWS account ID (ID da conta da AWS) mostra os IDs das contas dos consumidores que estão usando a Reserva de capacidade no momento. A coluna Launched instances (Instâncias executadas) mostra o número de instâncias que cada consumidor está executando na capacidade reservada no momento.

Para visualizar o uso da Reserva de capacidade usando a AWS CLI

Use o comando [get-capacity-reservation-usage](#). AccountId mostra o ID da conta que está usando a Reserva de capacidade. UsedInstanceCount mostra o número de instâncias de consumidor que estão executando na capacidade reservada no momento.

Permissões de Reserva de capacidade compartilhada

Permissões para proprietários

Os proprietários são responsáveis por gerenciar e cancelar suas Reservas de Capacidade compartilhadas. Os proprietários não podem modificar instâncias em execução na Reserva de capacidade compartilhada que sejam de propriedade de outras contas. Os proprietários continuam responsáveis pelo gerenciamento das instâncias que executam na Reserva de capacidade compartilhada.

Permissões para consumidores

Os consumidores são responsáveis pelo gerenciamento de suas instâncias que estão em execução na Reserva de capacidade compartilhada. Os consumidores não podem modificar a Reserva de capacidade compartilhada de nenhuma forma e não podem visualizar nem modificar instâncias que são de propriedade de outros consumidores ou do proprietário da Reserva de capacidade.

Faturamento e medição

Não há cobranças adicionais pelo compartilhamento de Reservas de Capacidade.

O proprietário da Reserva de capacidade é cobrado pelas instâncias que executa na Reserva de capacidade e pela capacidade reservada não utilizada. Os consumidores são cobrados pelas instâncias que executam na Reserva de capacidade compartilhada.

Limites de instâncias

Todo o uso da Reserva de capacidade é contado em relação aos limites de instância sob demanda do proprietário da Reserva de capacidade. Isso inclui:

- Capacidade reservada não utilizada
- Uso por instâncias de propriedade do proprietário da Reserva de capacidade
- Uso por instâncias de propriedade de consumidores

As instâncias executadas na capacidade reservada por consumidores são contadas em relação ao limite de instância sob demanda do proprietário da Reserva de capacidade. Os limites de instâncias dos consumidores são a soma de seus próprios limites de instância sob demanda e a capacidade disponível nas Reservas de Capacidade compartilhadas que podem acessar.

Métricas do CloudWatch para Reservas de Capacidade sob demanda

Com as métricas do CloudWatch, você pode monitorar as Reservas de Capacidade e identificar a capacidade não utilizada configurando os alarmes do CloudWatch para notificá-lo quando os limites de uso

forem atingidos. Isso pode ajudá-lo a manter um volume constante de Reserva de capacidade e atingir um nível mais alto de utilização.

As Reservas de Capacidade sob demanda enviam dados de métricas ao CloudWatch a cada cinco minutos. Não há suporte para métricas de Reservas de Capacidade que estejam ativas por menos de cinco minutos.

Para obter mais informações sobre como visualizar métricas no console do CloudWatch, consulte [Usar as métricas do Amazon CloudWatch](#). Para obter mais informações sobre como criar alarmes, consulte [Criar alarmes do Amazon CloudWatch](#).

Tópicos

- [Métricas de uso da Reserva de capacidade \(p. 411\)](#)
- [Dimensões de métricas da Reserva de capacidade \(p. 411\)](#)
- [Visualizar métricas do CloudWatch nas Reservas de Capacidade \(p. 411\)](#)

Métricas de uso da Reserva de capacidade

O namespace AWS/EC2CapacityReservations inclui as seguintes métricas de uso que você pode usar para monitorar e manter a capacidade sob demanda dentro dos limites especificados para sua reserva.

Métrica	Descrição
UsedInstanceCount	O número de instâncias que estão em uso no momento. Unidade: contagem
AvailableInstanceCount	O número de instâncias disponíveis. Unidade: contagem
TotalInstanceCount	O número total de instâncias reservadas. Unidade: contagem
InstanceUtilization	A porcentagem de instâncias de capacidade reservada que estão em uso no momento. Unidade: percentual

Dimensões de métricas da Reserva de capacidade

Você pode usar as seguintes dimensões para refinar as métricas listadas na tabela anterior.

Dimensão	Descrição
CapacityReservationId	Essa dimensão globalmente exclusiva filtra os dados solicitados somente para a reserva de capacidade identificada.

Visualizar métricas do CloudWatch nas Reservas de Capacidade

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, pelas várias dimensões com suporte. É possível usar os procedimentos a seguir para visualizar as métricas de suas Reservas de Capacidade.

Para visualizar as métricas da Reserva de capacidade usando o console do CloudWatch

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. Se necessário, altere a região. Na barra de navegação, selecione a região em que a Reserva de capacidade reside. Para obter mais informações, consulte [Regiões e endpoints](#).
3. No painel de navegação, selecione Metrics (Métricas).
4. Para Todas as métricas, escolha Reservas de Capacidade do EC2.
5. Escolha a dimensão da métrica Por reserva de capacidade. As métricas serão agrupadas por CapacityReservationId.
6. Para classificar a métrica, use o cabeçalho da coluna. Para criar um gráfico de uma métrica, marque a caixa de seleção ao lado da métrica.

Como visualizar métricas da Reserva de capacidade (AWS CLI)

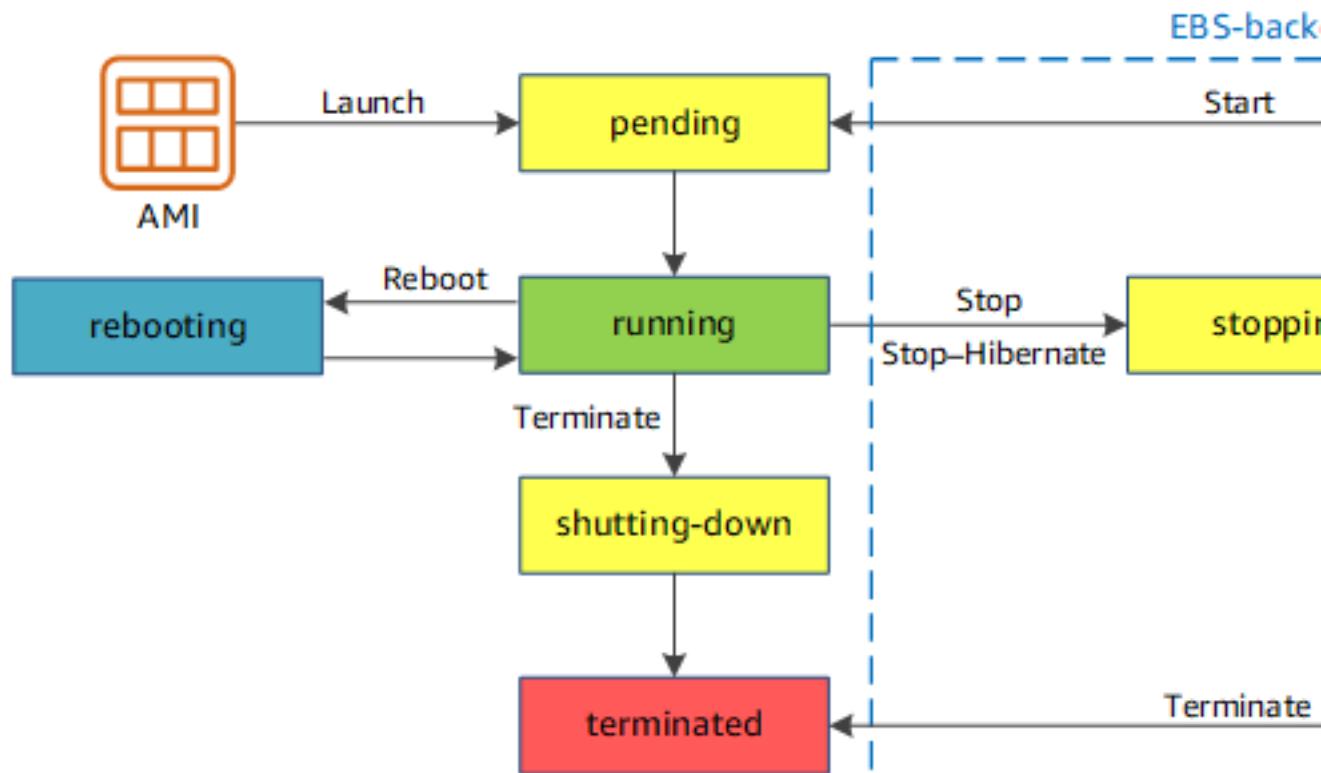
Use o comando `list-metrics` a seguir:

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Ciclo de vida da instância

Uma instância do Amazon EC2 passa por diferentes estados do momento em que você a inicia até seu encerramento.

A ilustração a seguir representa as transições entre os estados da instância.



A tabela a seguir fornece uma breve descrição de cada estado da instância e indica se ela foi faturada ou não.

Note

A tabela indica apenas o faturamento para uso da instância. Alguns recursos da AWS, como volumes do Amazon EBS e endereços IP elásticos, incorrem em cobranças independentemente do estado da instância. Para obter mais informações, consulte [Evitar cobranças inesperadas](#) no Manual do usuário do AWS Billing and Cost Management.

Estado da instância	Descrição	Faturamento para uso da instância
pending	A instância está se preparando para entrar no estado <code>running</code> . Uma instância entra no estado <code>pending</code> quando ela é executada pela primeira vez ou quando é iniciada após estar no estado <code>stopped</code> .	Não faturado
running	A instância está em execução e pronta para uso.	Faturado
stopping	A instância está se preparando para ser interrompida ou parar de hibernada.	Não faturada se estiver se preparando para interrupção Faturada se estiver se preparando para hibernação
stopped	A instância está desativada e não pode ser usada. A instância pode ser iniciada a qualquer momento.	Não faturado
shutting down	A instância está se preparando para ser encerrada.	Não faturado
terminated	Instância foi permanentemente excluída e não pode ser iniciada.	Não faturado Note As instâncias reservadas que foram aplicadas a instâncias encerradas são faturadas até o final do prazo de acordo com a opção de pagamento. Para obter mais informações, consulte Reserved Instances (p. 259)

Note

A reinicialização de uma instância não inicia um novo período de faturamento porque ela permanece no estado `running`.

Execução da instância

Quando você executa uma instância, ela entra no estado `pending`. O tipo de instância que você especificou na execução determina o hardware de computador host para sua instância. Usamos a imagem

de máquina da Amazon (AMI) especificada na execução para inicializar a instância. Depois de a instância estar pronta para você, ela entra no estado `running`. Você pode se conectar à instância em execução e usá-la da forma como usaria um computador bem à sua frente.

Assim que sua instância fizer a transição para o estado `running`, você será cobrado por cada segundo, com o mínimo de um minuto, que mantiver a instância em execução, mesmo se a instância permanecer ociosa e você não se conectar a ela.

Para obter mais informações, consulte [Executar sua instância \(p. 417\)](#) e [Conectar-se à sua instância do Windows \(p. 443\)](#).

Interrupção e início de instância (somente instâncias baseadas no Amazon EBS)

Se sua instância falhar na verificação de status ou não estiver executando suas aplicações como esperado, e se o volume do dispositivo raiz de sua instância for um volume do Amazon EBS, você poderá parar e iniciar a instância para tentar corrigir o problema.

Quando você para sua instância, ela entra no estado `stopping` e, em seguida, no estado `stopped`. Não cobramos pelo uso nem por taxas de transferência de dados da sua instância depois de você interrompê-la, mas cobramos pelo armazenamento dos volumes do Amazon EBS. Quando sua instância estiver no estado `stopped`, você poderá modificar determinados atributos da instância, inclusive o tipo de instância.

Quando você inicia a instância, ela entra no estado `pending` e a movemos para um novo computador host (embora em alguns casos, ela permaneça no host atual). Quando você para e inicia sua instância, perde todos os dados nos volumes de armazenamento da instâncias no computador host anterior.

Sua instância retém o endereço IPv4 privado, o que significa que um endereço IP elástico associado ao endereço IPv4 privado ou à interface de rede ainda estará associado à sua instância. Se sua instância tiver um endereço IPv6, ela reterá o endereço IPv6.

Toda vez que você faz a transição de uma instância de `stopped` para `running`, cobramos por segundo quando a instância está em execução, com no mínimo um minuto sempre que a instância é iniciada.

Para obter mais informações, consulte [Interromper e iniciar sua instância \(p. 455\)](#).

Hibernação de instância (somente instâncias baseadas no Amazon EBS)

Ao hibernar uma instância, sinalizamos para o sistema operacional para executar hibernação (`suspend-to-disk`), o que salva o conteúdo da memória da instância (RAM) no volume raiz do Amazon EBS. Persistimos o volume raiz do Amazon EBS e todos os volumes de dados do Amazon EBS da instância anexados. Quando você inicia a instância, o volume raiz do Amazon EBS é restaurado para seu estado anterior, e o conteúdo da RAM é recarregado. Os volumes de dados anexados anteriormente são reanexados e a instância conserva seu ID de instância.

Quando você hiberna a instância, ela entra no estado `stopping` e, em seguida, no estado `stopped`. Não cobramos pelo uso de uma instância hibernada quando ela está no estado `stopped`, mas cobramos quando ela está no estado `stopping`, ao contrário de quando você [interrompe uma instância \(p. 414\)](#) sem hiberná-la. Não cobramos pelo uso de taxas de transferência de dados, mas cobramos pelo armazenamento de qualquer volume do Amazon EBS, incluindo armazenamento dos dados da RAM.

Quando você inicia a instância hibernada, ela entra no estado `pending` e a movemos para um novo computador host (embora em alguns casos, ela permaneça no host atual).

Sua instância retém o endereço IPv4 privado, o que significa que um endereço IP elástico associado ao endereço IPv4 privado ou à interface de rede ainda estará associado à sua instância. Se sua instância tiver um endereço IPv6, ela reterá o endereço IPv6.

Para obter mais informações, consulte [Hibernar a instância do Linux sob demanda ou reservada \(p. 459\)](#).

Reinicialização da instância

Você pode reinicializar sua instância usando o console do Amazon EC2, uma ferramenta de linha de comando e a API do Amazon EC2. Recomendamos que você use o Amazon EC2 para reinicializar sua instância em vez de executar o comando de reinicialização do sistema operacional pela sua instância.

A reinicialização de uma instância equivale a reinicialização de um sistema operacional. A instância permanece no mesmo computador host e mantém seu nome DNS público, endereço IP privado e todos os dados em seus volumes de armazenamento de instância. Normalmente demora alguns minutos para a reinicialização ser concluída, mas o tempo necessário para reinicialização depende da configuração da instância.

Reiniciar uma instância não inicia uma novo período de faturamento de instância; o faturamento por segundo continua sem a cobrança mínima de um minuto.

Para obter mais informações, consulte [Reinicializar a instância \(p. 470\)](#).

Desativação da instância

A instância está programada para ser inativada quando a AWS detectar uma falha irreparável do hardware subjacente que a hospeda. Quando uma instância atinge sua data de desativação programada, ela é interrompida ou encerrada pela AWS. Se o dispositivo raiz da instância estiver em um volume do Amazon EBS, a instância será interrompida e você poderá reiniciá-la a qualquer momento. Se o dispositivo raiz da instância estiver em um volume de armazenamento de instâncias, a instância será encerrada e não poderá ser usada novamente.

Para obter mais informações, consulte [Desativação da instância \(p. 471\)](#).

Encerramento de instância

Ao perceber que não necessita mais de uma instância, pode encerrá-la. Assim que o estado de uma instância de mudar para `shutting-down` ou para `terminated`, não haverá mais custos para essa instância.

Se você ativou a proteção de encerramento, não poderá encerrar a instância usando o console, a CLI ou a API.

Depois de encerrar uma instância, ela permanecerá visível no console por um curto período, quando será automaticamente excluída. Você também pode descrever uma instância encerrada usando a CLI e a API. Recursos (como tags) são gradualmente dissociados da instância encerrada, portanto podem não ser visíveis na instância encerrada após um breve período. Você não pode se conectar nem recuperar uma instância encerrada.

Cada instância com Amazon EBS oferece suporte ao atributo `InstanceInitiatedShutdownBehavior`, que controla se instância é parada ou encerrada ao iniciar uma desativação de dentro da instância em si. O comportamento padrão é interromper a instância. Você pode modificar a configuração desse atributo enquanto a instância estiver sendo executada ou parada.

Cada volume do Amazon EBS oferece suporte ao atributo `DeleteOnTermination`, que controla se o volume é excluído ou preservado ao encerrar a instância à qual ela está associada. O padrão é excluir o volume do dispositivo raiz e preservar todos os outros volumes do EBS.

Para obter mais informações, consulte [Encerrar a instância \(p. 474\)](#).

Diferenças entre reinicialização, interrupção, hibernação e encerramento

A tabela a seguir resume as principais diferenças entre reinicialização, parada, hibernação e encerramento da sua instância.

Característica	Reiniciar	Parar/iniciar (somente instâncias com Amazon EBS)	Hibernação (somente instâncias baseadas em Amazon EBS)	Encerrar
Computador host	A instância permanece no mesmo computador host	Nós movemos a instância para um novo computador host (embora em alguns casos, ela permaneça no host atual).	Nós movemos a instância para um novo computador host (embora em alguns casos, ela permaneça no host atual).	Nenhum
Endereços IPv4 privados e públicos	Esses endereços permanecem iguais	A instância mantém seu endereço IPv4 privado. A instância obtém um endereço IPv4 público, a menos que tenha um endereço IP elástico, que não muda parada/inicialização.	A instância mantém seu endereço IPv4 privado. A instância obtém um endereço IPv4 público, a menos que tenha um endereço IP elástico, que não muda parada/inicialização.	Nenhum
Endereços IP elásticos (IPv4)	O endereço IP elástico permanece associado à instância	O endereço IP elástico permanece associado à instância	O endereço IP elástico permanece associado à instância	O endereço IP elástico está dissociado da instância
Endereço IPv6	O endereço permanece o mesmo	A instância mantém seu endereço IPv6	A instância mantém seu endereço IPv6	Nenhum
Volumes de armazenamento de instâncias	Os dados são preservados	Os dados são apagados	Os dados são apagados	Os dados são apagados
Volume do dispositivo raiz	O volume é preservado	O volume é preservado	O volume é preservado	O volume é excluído por padrão
RAM (conteúdo da memória)	A RAM é apagada	A RAM é apagada	A RAM é salva em um arquivo no volume raiz	A RAM é apagada
Faturamento	A hora de fatura da instância não é alterada.	As cobranças de uma instância são interrompidas assim que o estado mudar para stopping.	Você incorre em cobranças quando a instância está no estado stopping, mas não incorre em	As cobranças de uma instância são interrompidas assim que o

Característica	Reiniciar	Parar/iniciar (somente instâncias com Amazon EBS)	Hibernação (somente instâncias baseadas em Amazon EBS)	Encerrar
		Toda vez que uma instância faz a transição de <code>stopped</code> para <code>running</code> , nós iniciamos um novo período, cobrando o mínimo de um minuto toda vez que você inicia a instância.	cobranças quando a instância está no estado <code>stopped</code> . Toda vez que uma instância faz a transição de <code>stopped</code> para <code>running</code> , nós iniciamos um novo período, cobrando o mínimo de um minuto toda vez que você inicia a instância.	estado mudar para <code>shutting-down</code> .

Os comandos de desligamento do sistema operacional sempre encerra uma instância com armazenamento de instâncias. Você pode controlar se os comandos de desativação do sistema operacional param ou encerram uma instância com Amazon EBS. Para obter mais informações, consulte [Alterar o comportamento de desligamento iniciado da instância \(p. 477\)](#).

Executar sua instância

Uma instância é um servidor virtual na Nuvem AWS. Você executa uma instância a partir de uma imagem de máquina da Amazon (AMI). A AMI fornece o sistema operacional, o servidor de aplicações e as aplicações para sua instância.

Ao se cadastrar na AWS, você poderá começar a usar o Amazon EC2 gratuitamente usando o [Nível gratuito da AWS](#). Você pode usar o nível gratuito para iniciar e usar uma instância `t2.micro` gratuitamente por 12 meses (em regiões onde `t2.micro` não estiver disponível, você poderá usar uma instância `t3.micro` no nível gratuito). Se você executar uma instância que não esteja no nível gratuito, serão cobradas as taxas de uso padrão do Amazon EC2 para a instância. Para obter mais informações, consulte [Definição de preço do Amazon EC2](#).

Você pode executar uma instância usando os métodos a seguir.

Método	Documentação
[Console do Amazon EC2] Use o assistente de execução de instância para especificar os parâmetros de execução.	É possível executar uma instância usando o assistente de execução de instância. (p. 419)
[Console do Amazon EC2] Crie um modelo de execução e execute a instância a partir desse modelo.	Executar uma instância a partir de um modelo de execução (p. 425)
[Console do Amazon EC2] Use uma instância existente como base.	Executar uma instância usando parâmetros de uma instância existente (p. 440)
[Console do Amazon EC2] Use uma AMI comprada do AWS Marketplace .	Executar uma instância AWS Marketplace (p. 441)
[AWS CLI] Use uma AMI selecionada.	Usar o Amazon EC2 pela AWS CLI
[AWS Tools for Windows PowerShell] Use uma AMI selecionada.	Amazon EC2 pela AWS Tools for Windows PowerShell

Método	Documentação
[AWS CLI] Use a EC2 Fleet para provisionar capacidade em diferentes tipos de instância do EC2 e zonas de disponibilidade, e em modelos de compra de instância sob demanda, instância reservada e instância spot.	EC2 Fleet (p. 712)
[AWS CloudFormation] Use um modelo de AWS CloudFormation para especificar uma instância.	AWS::EC2::Instance no Manual do usuário do AWS CloudFormation
[AWS SDK] Use um SDK específico de idioma da AWS para executar uma instância.	AWS SDK for .NET da AWS SDK para C++ AWS SDK para Go AWS SDK para Java AWS SDK para JavaScript AWS SDK para PHP V3 AWS SDK for Python AWS SDK para Ruby V3

Ao executar a instância, você pode executá-la em uma sub-rede associada a um dos seguintes recursos:

- Uma zona de disponibilidade – esta opção é o padrão.
- Uma Local Zone: para executar uma instância em uma Local Zone, você deve optar pela Local Zone e criar uma sub-rede na zona. Para obter mais informações, consulte [Local Zones](#).
- Uma zona de Wavelength: para executar uma instância em uma zona de Wavelength, opte pela zona de Wavelength e crie uma sub-rede na zona. Para obter informações sobre como executar uma instância em uma zona do Wavelength, consulte [Conceitos básicos do AWS Wavelength](#) no Guia do desenvolvedor do AWS Wavelength.
- Um Outpost – para executar uma instância em um Outpost, é necessário criar um Outpost. Para obter informações sobre como criar um Outpost, consulte [Get Started with \(Conceitos básicos do Outpost\)AWS Outposts](#) no AWS Outposts Guia do Usuário.

Após executar a instância, você pode conectar-se a ela e usá-la. Para começar, o estado da instância é `pending`. Quando o estado de instância for `running`, a instância terá começado a inicialização. Pode passar um breve tempo antes de você se conectar à instância. Observe que os tipos de instância bare metal podem levar mais tempo para serem executados. Para obter mais informações sobre instâncias bare metal, consulte [Instâncias criadas no Sistema Nitro \(p. 154\)](#).

A instância recebe um nome DNS público que você pode usar para contatar a instância pela Internet. A instância também recebe um nome DNS privado que outras instâncias na mesma VPC podem usar para contatar a instância. Para obter mais informações sobre como se conectar à sua instância, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).

Quando você tiver terminado com uma instância, encerre-a. Para obter mais informações, consulte [Encerrar a instância \(p. 474\)](#).

É possível executar uma instância usando o assistente de execução de instância.

É possível executar uma instância usando o assistente de execução de instância. O assistente de execução de instância especifica todos os parâmetros de execução necessários para executar uma instância. Quando o assistente de execução de instância fornece um valor padrão, é possível aceitá-lo ou especificar seu próprio valor. No mínimo, você precisa selecionar uma AMI e um par de chaves para executar uma instância.

Antes de executar a instância, verifique se está configurado. Para obter mais informações, consulte [Configuração para usar o Amazon EC2. \(p. 6\)](#).

Important

Quando você executa uma instância que não esteja dentro do [Nível gratuito da AWS](#), será cobrado pelo tempo que a instância é executada, mesmo se ela permanecer inativa.

Etapas para executar uma instância:

- [Iniciar a execução da instância \(p. 419\)](#)
- [Etapa 1: Escolher uma imagem de máquina da Amazon \(AMI\) \(p. 419\)](#)
- [Etapa 2: escolher um tipo de instância \(p. 420\)](#)
- [Etapa 3: configurar detalhes da instância \(p. 421\)](#)
- [Etapa 4: adicionar armazenamento \(p. 423\)](#)
- [Etapa 5: Adicionar tags \(p. 424\)](#)
- [Etapa 6: configurar o grupo de segurança \(p. 424\)](#)
- [Etapa 7: Revisar a execução da instância e selecionar o par de chaves \(p. 425\)](#)

Iniciar a execução da instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação na parte superior da tela, a região atual será exibida (por exemplo, US East (Ohio)). Selecione uma região para a instância que atenda às suas necessidades. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre Regiões, enquanto outros não podem. Para obter mais informações, consulte [Localizações de recursos \(p. 1544\)](#).
3. No painel do console do Amazon EC2, selecione Launch instance (Executar instância).

Etapa 1: Escolher uma imagem de máquina da Amazon (AMI)

Quando você executa uma instância, deve selecionar uma configuração, conhecida como imagem de máquina da Amazon (AMI). A AMI contém as informações necessárias para criar uma nova instância. Por exemplo, uma AMI pode conter o software necessário para atuar como servidor Web, por exemplo, Windows, Apache e seu site.

Ao iniciar uma instância, é possível selecionar uma AMI na lista ou selecionar um parâmetro do Systems Manager que aponte para o ID de uma AMI. Para obter mais informações, consulte [Usar um parâmetro do Systems Manager para localizar uma AMI](#).

Na página Choose an Amazon Machine Image (AMI) (Escolher uma imagem de máquina da Amazon (AMI)), use uma das duas opções para escolher uma AMI. [pesquisar a lista de AMIs \(p. 419\)](#) ou [pesquisar por parâmetro do Systems Manager \(p. 420\)](#).

Pesquisando a lista de AMIs

1. Selecione o tipo de AMI para usar no painel esquerdo:

Início rápido

Uma seleção de AMIs populares para ajudá-lo a começar rapidamente. Para selecionar um AMI qualificado para o nível gratuito, escolha Free tier only (Somente nível gratuito) no painel à esquerda. Essas AMIs estão marcadas como Free tier eligible (Elegíveis para nível gratuito).

Minhas AMIs

As AMIs privadas que você possui, ou as AMI privadas que foram compartilhadas com você. Para visualizar as AMIs compartilhadas com você, selecione Shared with me (Compartilhadas comigo) no painel esquerdo.

AWS Marketplace

Uma loja online onde você pode comprar software executado na AWS, inclusive AMIs. Para obter mais informações sobre como executar uma instância pelo AWS Marketplace , consulte [Executar uma instância AWS Marketplace \(p. 441\)](#).

AMIs da comunidade

Os AMIs que os membros da comunidade AWS disponibilizaram para outras pessoas usarem. Para filtrar a lista de AMI por sistema operacional, marque a caixa apropriada em Operating system (Sistema operacional). Você também pode filtrar por arquitetura e tipo de dispositivo raiz.

2. Verifique o Virtualization type (Tipo de virtualização) listado para cada AMI. Observe que as AMIs são do tipo de que você precisa, seja hvm ou paravirtual. Por exemplo, alguns tipos de instância exigem HVM.
3. Verifique o modo de inicialização listado para cada AMI. Observe quais AMIs usam o modo de inicialização que você precisa, legacy-bios ou uefi. Para obter mais informações, consulte [Modos de inicialização \(p. 22\)](#).
4. Escolha a AMI que atenda às suas necessidades e marque Select (Selecionar).

Por parâmetro do Systems Manager

1. Escolha Search by Systems Manager parameter (Pesquisar por parâmetro do Systems Manager) (no canto superior direito).
2. Em Systems Manager parameter (Parâmetro do Systems Manager), selecione um parâmetro. O ID da AMI correspondente é exibido ao lado de Currently resolves to (Resolve atualmente para).
3. Escolha Pesquisar. As AMIs correspondentes ao ID da AMI são exibidas na lista.
4. Selecione a AMI na lista e escolha Select (Selecionar).

Etapa 2: escolher um tipo de instância

Na página Choose an Instance Type (Escolher um tipo de instância), selecione a configuração do hardware e o tamanho da instância a ser executada. Os tipos de instâncias maiores têm mais CPU e memória. Para obter mais informações, consulte [Tipos de instância \(p. 149\)](#).

Para permanecer qualificado para o nível gratuito, escolha o tipo de instância t2.micro (ou o tipo de instância t3.micro em regiões onde t2.micro não estiver disponível). Para obter mais informações, consulte [Instâncias expansíveis \(p. 169\)](#).

Por padrão, o assistente exibe tipos de instância da geração atual e seleciona o primeiro tipo de instância disponível com base na AMI selecionada. Para ver os tipos de instância de geração anterior, escolha All generations (Todas as gerações) na lista de filtros.

Note

Como configurar uma instância rapidamente para fins de teste, escolha Review and Launch (Revisar e executar) para aceitar as configurações padrão e executar a instância. Caso contrário,

para configurar sua instância ainda mais, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).

Etapa 3: configurar detalhes da instância

Na página Configure Instance Details (Configurar detalhes da instância), altere as configurações a seguir conforme necessário (expanda Advanced Details (Detalhes avançados) para visualizar todas as configurações) e selecione Next: Add Storage (Próximo: Adicionar armazenamento):

- Number of instances (Número de instâncias): Digite o número de instâncias para executar.

Tip

Para garantir uma execução mais rápida da instância, divida solicitações grandes em lotes menores. Por exemplo, crie cinco solicitações de execução separadas para 100 instâncias cada em vez de uma solicitação de execução para 500 instâncias.

- (Opcional) Para ajudar a assegurar que você mantenha o número de instâncias para lidar com a demanda do aplicativo, escolha Launch into Auto Scaling Group (Executar no grupo de Auto Scaling) para criar uma configuração de execução e um grupo de Auto Scaling. O Auto Scaling escala o número de instâncias no grupo de acordo com suas especificações. Para mais informações, consulte o [Guia do usuário do Amazon EC2 Auto Scaling](#).

Note

Se o Amazon EC2 Auto Scaling marcar uma instância que está em um grupo do Auto Scaling como não íntegro, a instância será programada automaticamente para substituição quando for encerrada e outra for iniciada, e você perderá os dados na instância original. Uma instância será marcada como não íntegra se você parar ou reiniciar a instância, ou se outro evento marcar a instância como não íntegra. Para obter mais informações, consulte [Verificações de integridade de instâncias do Auto Scaling](#) no Guia do usuário do Amazon EC2 Auto Scaling.

- Purchasing option (Opção de compra): escolha Request Spot instances (Solicitar instâncias spot) para executar uma instância Spot. Isso adiciona e remove opções desta página. Defina o preço máximo e, se desejar, atualize o tipo de solicitação, o comportamento da interrupção e a validade da solicitação. Para obter mais informações, consulte [Criar uma solicitação de instância spot \(p. 313\)](#).
- Rede social: selecione a VPC ou para criar uma nova VPC, selecione Create new VPC (Criar nova VPC) para acessar o console do Amazon VPC. Quando tiver concluído, retorne ao assistente e escolha Refresh (Atualizar) para carregar sua VPC na lista.
- Subnet (Sub-rede): você pode executar uma instância em uma sub-rede associada a uma zona de disponibilidade, a uma Local Zone, a uma zona de Wavelength ou a um Outpost.

Para executar a instância em uma zona de disponibilidade, selecione a sub-rede na qual a instância será executada. Você pode selecionar No preference (Sem preferência) para deixar a AWS escolher uma sub-rede padrão em alguma zona de disponibilidade. Para criar uma nova sub-rede, escolha Create new subnet (Criar nova sub-rede) para acessar o console da Amazon VPC. Quando tiver concluído, retorne ao assistente e escolha Refresh (Atualizar) para carregar sua sub-rede na lista.

Para iniciar a instância em uma Local Zone, selecione uma sub-rede que você criou na Local Zone.

Para executar uma instância em um Outpost, selecione uma sub-rede em uma VPC associada a um Outpost.

- Auto-assign Public IP (Autoatribuir IP público): especifique se sua instância recebe um endereço IPv4 público. Por padrão, as instâncias em uma sub-rede padrão recebem um endereço IPv4 público e as instâncias em uma sub-rede não padrão, não. Selecione Enable (Habilitar) ou Disable (Desabilitar) para substituir a configuração padrão da sub-rede. Para obter mais informações, consulte [Endereços IPv4 públicos e nomes de host DNS externos \(p. 957\)](#).
- Auto-assign IPv6 IP (Autoatribuir IP do IPv6): especifique se sua instância recebe um endereço IPv6 do intervalo da sub-rede. Selecione Enable (Habilitar) ou Disable (Desabilitar) para substituir a configuração padrão da sub-rede. Essa opção só estará disponível se você tiver associado um bloco CIDR IPv6 com

sua VPC e sub-rede. Para obter mais informações, consulte [Sua VPC e suas sub-redes](#) em Guia do usuário da Amazon VPC.

- Domain join directory (Diretório de junção de domínio): selecione o diretório AWS Directory Service (domínio) ao qual sua instância do Windows está unida após a execução. Se selecionar um domínio, você deve selecionar a função do IAM com as permissões necessárias. Para obter mais informações, consulte [Associe continuamente uma instância do EC2 do Windows](#).
- Placement group (Grupo de posicionamento): um grupo de posicionamento determina a estratégia de posicionamento das instâncias. Selecione um grupo de posicionamento existente ou crie um novo. Essa opção só estará disponível se você tiver selecionado um tipo de instância que ofereça suporte aos grupos de posicionamento. Para obter mais informações, consulte [Grupos de posicionamento \(p. 1044\)](#).
- Reserva de capacidade: especifique se deseja executar a instância em capacidade compartilhada, qualquer Reserva de capacidade open, uma Reserva de capacidade específica ou um grupo de Reserva de capacidade. Para obter mais informações, consulte [Iniciar instâncias em uma Reserva de capacidade existente \(p. 400\)](#).
- IAM role (Função do IAM): selecione a função do AWS Identity and Access Management (IAM) para associar à instância. Para obter mais informações, consulte [Funções do IAM para Amazon EC2 \(p. 1195\)](#).
- CPU options (Opções de CPU): escolha Specify CPU options (Especificar opções de CPU) para especificar um número personalizado de vCPUs durante a execução. Defina o número de núcleos de CPU e de threads por núcleo. Para obter mais informações, consulte [Otimizar as opções de CPU \(p. 582\)](#).
- Shutdown behavior (Comportamento de desativação): selecione se a instância deve parar ou encerrar quando desativada. Para obter mais informações, consulte [Alterar o comportamento de desligamento iniciado da instância \(p. 477\)](#).
- Stop - Hibernate behavior (Interromper - comportamento de hibernação): para habilitar a hibernação, marque essa caixa de seleção. Essa opção só estará disponível se a instância atender aos pré-requisitos de hibernação. Para obter mais informações, consulte [Hibernar a instância do Linux sob demanda ou reservada \(p. 459\)](#).
- Enable termination protection (Permitir proteção de encerramento): para evitar o encerramento acidental, marque esta caixa de seleção. Para obter mais informações, consulte [Habilitar a proteção contra encerramento \(p. 476\)](#).
- Monitoring (Monitoramento): marque essa caixa de seleção para ativar o monitoramento detalhado da sua instância usando o Amazon CloudWatch. Aplicam-se cobranças adicionais. Para obter mais informações, consulte [Monitorar instâncias usando o CloudWatch \(p. 898\)](#).
- EBS-Optimized instance (Instância otimizada para EBS): uma instância otimizada para Amazon EBS usa uma pilha de configuração otimizada e fornece capacidade dedicada adicional para E/S do Amazon EBS. Se o tipo de instância é compatível com esse recurso, marque esta caixa de seleção pra habilitá-lo. Aplicam-se cobranças adicionais. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).
- Tenancy (Alocação): se você estiver executando a instância em uma VPC, poderá optar por executar a instância em hardware isolado e dedicado (Dedicated - Dedicado) ou em um host dedicado (Dedicated host - Host dedicado). Podem se aplicar cobranças adicionais. Para obter mais informações, consulte [Dedicated Instances \(p. 383\)](#) e [Dedicated Hosts \(p. 349\)](#).
- T2/T3 Unlimited (T2/T3 ilimitado): marque essa caixa de seleção para permitir que as aplicações tenham intermitência acima da linha de base pelo tempo que for necessário. Podem se aplicar cobranças adicionais. Para obter mais informações, consulte [Instâncias expansíveis \(p. 169\)](#).
- Network interfaces (Interfaces de rede): se você tiver selecionado uma sub-rede específica, pode especificar até duas interfaces de rede para sua instância:
 - Para Network Interface (Interface de rede), selecione New network interface (Nova interface de rede) para deixar a AWS criar uma interface nova ou selecione uma interface de rede existente e disponível.
 - Para Primary IP (IP primário), insira um endereço IPv4 privado do intervalo da sua sub-rede ou deixe Auto-assign (Atribuir automaticamente) para deixar a AWS escolher um endereço IPv4 privado para você.

- Para Secondary IP addresses (Endereços IP secundários), escolha Add IP (Adicionar IP) para atribuir mais de um endereço IPv4 privado à interface de rede selecionada.
- (Somente IPv6) Para IPs IPv6, escolha Add IP (Adicionar IP) e digite um endereço IPv6 do intervalo da sub-rede ou deixe como Auto-assign (Autoatribuir) permitir que a AWS escolha um para você.
- Network Card Index (Índice da placa de rede): O índice da placa de rede. A interface de rede primária deve ser atribuída ao índice 0 da placa de rede. Alguns tipos de instância suportam várias placas de rede.
- Selecione Add Device (Adicionar dispositivo) para adicionar uma interface de rede secundária. Uma interface de rede secundária pode residir em uma sub-rede diferente da VPC, pois está na mesma zona de disponibilidade que sua instância.

Para obter mais informações, consulte [Interfaces de rede elástica \(p. 1002\)](#). Se você especificar mais de uma interface de rede, sua instância não poderá receber um endereço IPv4 público. Além disso, se você especificar uma interface de rede existente para eth0, não poderá substituir a configuração de IPv4 pública da sub-rede usando Auto-assign Public IP (Atribuir IP público automaticamente). Para obter mais informações, consulte [Atribuir um endereço IPv4 público durante a execução da instância \(p. 961\)](#).

- Kernel ID (ID do kernel): (válido somente para AMIs paravirtuais (PV)) selecione Use default (Usar padrão), a menos que deseje usar um kernel específico.
- RAM disk ID (ID do disco de RAM): (válido somente para AMIs paravirtuais (PV)) selecione Use default (Usar padrão), a menos que deseje usar um disco RAM específico. Se você tiver selecionado um kernel, pode precisar selecionar um disco de RAM específico com os drivers para oferecer suporte a ele.
- Enclave: selecione Enable (Ativar) para ativar a instância para o AWS Nitro Enclaves. Para obter mais informações, consulte [O que é o AWS Nitro Enclaves?](#) no Guia do usuário do AWS Nitro Enclaves.
- Metadata accessible (Metadados acessíveis): você pode habilitar ou desabilitar o acesso aos metadados da instância. Para obter mais informações, consulte [Usar IMDSv2 \(p. 623\)](#).
- Transporte de metadados: você pode habilitar ou desabilitar o método de acesso ao serviço de metadados de instância que está disponível para essa instância do EC2 com base no tipo de endereço IP (IPv4, IPv6 ou IPv4 e IPv6) da instância. Para obter mais informações, consulte [Recuperar metadados da instância \(p. 630\)](#).
- Metadata version (Versão de metadados): se você habilitar o acesso aos metadados da instância, poderá optar por exigir o uso do Serviço de metadados da instância versão 2 ao solicitar metadados da instância. Para obter mais informações, consulte [Configurar opções de metadados da instância para novas instâncias \(p. 627\)](#).
- Metadata token response hop limit (Limite de salto de resposta do token de metadados): se você habilitar metadados de instância, poderá definir o número permitido de saltos de rede para o token de metadados. Para obter mais informações, consulte [Usar IMDSv2 \(p. 623\)](#).
- User data (Dados do usuário): você pode especificar dados do usuário para configurar uma instância durante a execução ou para executar um script de configuração. Para associar um arquivo, selecione a opção As file (Como arquivo) e procure o arquivo a ser associado.

Etapa 4: adicionar armazenamento

A AMI que você selecionou inclui um ou mais volumes de armazenamento, incluindo o volume de dispositivo raiz. Na página Add Storage (Adicionar armazenamento), especifique os volumes adicionais para anexar à instância escolhendo Add New Volume (Adicionar novo volume). Configure cada volume conforme a seguir e escolha Next: Add Tags (Próximo: Adicionar tags).

- Type (Tipo): selecione os volumes de armazenamento de instâncias ou do Amazon EBS para associar à instância. Os tipos de volume disponíveis na lista dependem do tipo de instância escolhido. Para obter mais informações, consulte [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#) e [Volumes do Amazon EBS \(p. 1245\)](#).
- Device (Dispositivo): selecione a lista de nomes de dispositivo disponíveis para o volume.

- **Snapshots:** digite o nome ou o ID do snapshot do qual deseja restaurar um volume. Você também pode pesquisar snapshots públicos e compartilhados que estão disponíveis digitando o texto no campo Snapshot. As descrições do snapshot diferenciam maiúsculas de minúsculas.
- **Size (Tamanho):** para volumes do EBS, especifique um tamanho de armazenamento. Mesmo se você tiver selecionado uma AMI e uma instância que estejam qualificadas para o nível gratuito, para permanecer no nível gratuito, seu armazenamento total deverá ficar abaixo de 30 GiB. Para obter mais informações, consulte [Restrições de tamanho e configuração de um volume do EBS \(p. 1265\)](#).
- **Volume Type (Tipo de volume):** para volumes do EBS, selecione um tipo de volume. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#).
- **IOPS:** se tiver selecionado um tipo de volume Provisioned IOPS SSD, você poderá inserir o número de operações de E/S por segundo (IOPS) ao qual o volume pode oferecer suporte.
- **Delete on Termination (Excluir ao finalizar):** para volumes do Amazon EBS, marque esta caixa para excluir o volume quando a instância for encerrada. Para obter mais informações, consulte [Preservar volumes do Amazon EBS no encerramento da instância \(p. 478\)](#).
- **Encrypted (Criptografado):** se o tipo de instância oferecer suporte à criptografia do EBS, você poderá especificar o estado de criptografia do volume. Se tiver habilitado a criptografia por padrão nessa região, a chave gerenciada pelo cliente padrão será selecionada para você. Você poderá selecionar uma chave diferente ou desabilitar a criptografia. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).

Etapa 5: Adicionar tags

Na página Add Tags (Adicionar tags), especifique as [tags \(p. 1554\)](#) fornecendo combinações de chave e valor. Você pode marcar a instância, os volumes ou ambos com uma tag. Para instâncias spot, você pode marcar apenas a solicitação de instância spot. Escolha Add another tag (Adicionar outra tag) para adicionar mais de uma tag aos seus recursos. Escolha Next: Configure Security Group ao concluir.

Etapa 6: configurar o grupo de segurança

Na página Configurar grupo de segurança, use um grupo de segurança para definir regras do firewall para sua instância. Essas regras especificam qual tráfego de rede de entrada será fornecido para sua instância. Todo o tráfego é ignorado. (Para mais informações sobre security groups, consulte [Grupos de segurança do Amazon EC2 para instâncias do Windows \(p. 1217\)](#).) Selecione ou crie um grupo de segurança da forma a seguir e escolha Review and Launch (Revisar e executar).

- Para selecionar um grupo de segurança existente, escolha Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança. (Opcional) Não é possível editar as regras de um grupo de segurança existente, mas é possível copiá-las a um novo grupo escolhendo Copy to new (Copiar para novo). Em seguida, adicione as regras conforme descrito na próxima etapa.
- Para criar um novo grupo de segurança, escolha Create a new security group (Criar um novo grupo de segurança). O assistente define automaticamente o grupo de segurança launch-wizard-x e cria uma regra de entrada para permitir que você se conecte à instância via RDP (porta 3389).
- Você pode adicionar regras de acordo com suas necessidades. Por exemplo, se a instância for um servidor Web, abra as portas 80 (HTTP) e 443 (HTTPS) para permitir o tráfego de Internet.

Para adicionar uma regra, escolha Add Rule (Adicionar regra), selecione o protocolo para abrir o tráfego de rede e especifique a origem. Escolha My IP (Meu IP) na lista Source (Origem) para deixar o assistente adicionar o endereço IP público do seu computador. No entanto, se você estiver se conectando por meio de um ISP ou por trás de um firewall sem um endereço IP estático, precisará encontrar o intervalo de endereços IP usado pelos computadores clientes.

Warning

Regras que permitem que todos os endereços IP (0.0.0.0/0) acessem a instância via SSH ou RDP são aceitáveis neste exercício rápido, mas não são seguras para ambientes

de produção. Você deve autorizar apenas um endereço IP específico ou um intervalo de endereços a acessar a instância.

Etapa 7: Revisar a execução da instância e selecionar o par de chaves

Na página Review Instance Launch (Revisar execução da instância), verifique os detalhes da sua instância e faça qualquer alteração necessária selecionando o link Edit (Editar) apropriado.

Quando estiver pronto, escolha Launch (Executar).

Na caixa de diálogo Select an existing key pair or create a new key pair (Selecionar um par de chaves existente ou criar um novo par de chaves), você poderá escolher um par de chaves existente ou poderá criar um novo. Por exemplo, selecione Choose an existing key pair (Escolha um par de chaves existente) e selecione o par de chaves que você criou para obter configuração. Para obter mais informações, consulte [Pares de chaves do Amazon EC2 e instâncias do Windows \(p. 1209\)](#).

Important

Se você escolher a opção Proceed without key pair (Continuar sem par de chaves), não conseguirá se conectar à instância a menos que escolha uma AMI configurada para permitir aos usuários uma maneira efetuar login.

Para executar uma instância, selecione a caixa de confirmação e escolha Launch Instances (Executar instâncias).

(Opcional) Você pode criar um alarme de verificação de status para a instância (taxas adicionais podem ser aplicadas). (Se você não tiver certeza, sempre pode adicionar um depois.) Na tela de confirmação, escolha Create status check alarms (Criar alarmes de verificação de status) e siga as instruções. Para obter mais informações, consulte [Criar e editar alarmes de verificação de status \(p. 872\)](#).

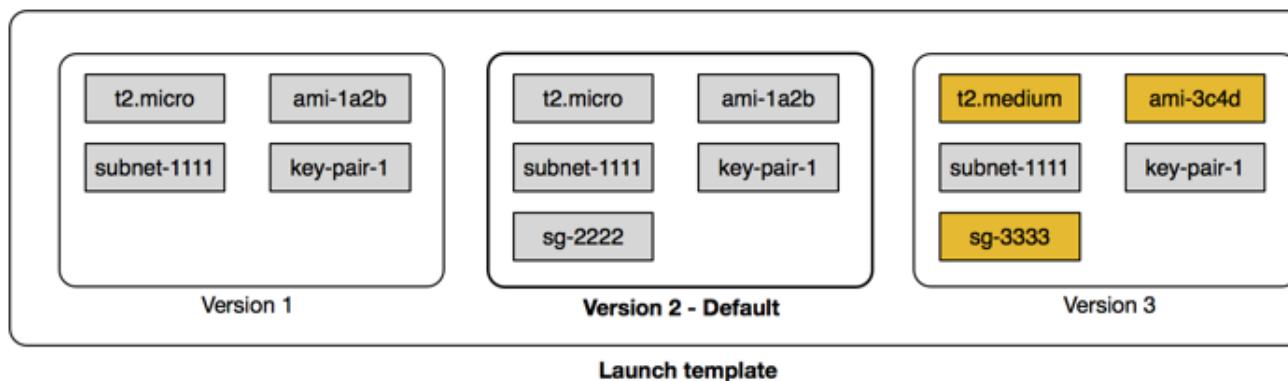
Se a instância não executar ou o estado passar imediatamente para terminated, em vez de running, consulte [Solucionar problemas de execução de instâncias \(p. 1570\)](#).

Executar uma instância a partir de um modelo de execução

Você pode criar um modelo de execução que contenha informações de configuração para executar uma instância. Você pode usar os modelos de inicialização para armazenar parâmetros de inicialização de modo que não precise especificá-los toda vez que iniciar uma instância. Por exemplo, um modelo de execução pode conter o ID da AMI, o tipo de instância e as configurações de rede que você geralmente usa para executar instâncias. Ao executar uma instância usando o console do Amazon EC2, a um AWS SDK ou uma ferramenta de linha de comando, você pode especificar o modelo de execução a ser usado.

Para cada modelo de execução, você pode criar uma ou mais versões de modelo de execução numeradas. Cada versão pode ter diferentes parâmetros de execução. Ao executar uma instância a partir de um modelo de execução, você poderá usar qualquer versão do modelo de execução. Se você não especificar uma versão, a versão padrão será usada. Você pode definir qualquer versão do modelo de execução como a versão padrão — por padrão, ela é a primeira versão do modelo de execução.

O diagrama a seguir mostra um modelo de execução com três versões. A primeira versão especifica o tipo de instância, o ID da AMI, a sub-rede e o par de chaves a ser usado para executar a instância. A segunda versão baseia-se na primeira versão e também especifica um security group para a instância. A terceira versão usa valores diferentes para alguns parâmetros. A versão 2 é definida como a versão padrão. Se você tiver executado uma instância a partir desse modelo de execução, os parâmetros de execução da versão 2 serão usados caso nenhuma outra versão tenha sido especificada.



Tópicos

- [Restrições do modelo de execução \(p. 426\)](#)
- [Uso de modelos de execução para controlar parâmetros de execução \(p. 427\)](#)
- [Controlar o uso dos modelos de execução \(p. 427\)](#)
- [Criar um modelo de execução \(p. 427\)](#)
- [Modificar um modelo de inicialização \(gerenciar versões do modelo de inicialização\) \(p. 434\)](#)
- [Executar uma instância a partir de um modelo de execução \(p. 437\)](#)
- [Usar modelos de execução com o Amazon EC2 Auto Scaling \(p. 438\)](#)
- [Usar modelos de execução com o Frota do EC2 \(p. 439\)](#)
- [Usar modelos de execução com a frota spot \(p. 439\)](#)
- [Excluir um modelo de execução \(p. 439\)](#)

Restrições do modelo de execução

As seguintes regras se aplicam aos modelos de execução e às respectivas versões:

- Você está limitado a criar 5.000 modelos de execução por região e 10.000 versões por modelo de execução.
- Os parâmetros do modelo de execução são opcionais. No entanto, você precisa garantir que sua solicitação de execução de uma instância inclui todos os parâmetros necessários. Por exemplo, se o modelo de execução não inclui um ID de AMI, você deverá especificar o modelo de execução e um ID de AMI ao executar uma instância.
- Os parâmetros do modelo de execução não são totalmente validados quando ele é criado. Se você especificar valores incorretos para parâmetros, ou se não usar combinações de parâmetro compatíveis, nenhuma instância poderá ser iniciada usando esse modelo de execução. Verifique se você especificou os valores corretos para os parâmetros e usou combinações de parâmetro compatíveis. Por exemplo, para executar uma instância em um grupo de posicionamento, especifique um tipo de instância compatível.
- Você pode marcar um modelo de execução, mas não pode marcar uma versão de modelo de execução.
- Os modelos de inicialização são imutáveis. Para modificar um modelo de inicialização, é necessário criar uma nova versão do modelo de inicialização.
- As versões de modelo de execução são numeradas na ordem em que são criadas. Ao criar uma versão de modelo de execução, você não pode especificar o número de versão por conta própria.

Uso de modelos de execução para controlar parâmetros de execução

Um modelo de execução pode conter todos ou alguns parâmetros para executar uma instância. Quando executa uma instância usando um modelo de execução, você pode substituir os parâmetros especificados no modelo de execução. Ou pode especificar parâmetros adicionais que não estão no modelo de execução.

Note

Você não pode remover os parâmetros do modelo de execução durante a execução (por exemplo, você não pode especificar um valor nulo para o parâmetro). Para remover um parâmetro, crie uma nova versão do modelo de execução sem o parâmetro e use essa versão para executar a instância.

Para executar instâncias, os usuários do IAM devem ter permissões para usar a ação `ec2:RunInstances`. Os usuários do IAM também devem ter permissões para criar ou usar recursos que são criados ou estão associados à instância. Você pode usar permissões em nível de recurso para a ação `ec2:RunInstances` para controlar os parâmetros de execução que podem ser especificados pelos usuários. Como alternativa, você pode conceder permissões aos usuários para executar uma instância usando um modelo de execução. Isso permite que você gerencie parâmetros de execução em um modelo de execução, em vez de uma política do IAM, e use um modelo de execução como um veículo de autorização para executar instâncias. Por exemplo, você pode especificar que os usuários só podem executar instâncias usando um modelo de execução e só podem usar um modelo de execução específico. Você também pode controlar os parâmetros de execução que os usuários podem substituir no modelo de execução. Para obter exemplos de políticas de , consulte [Modelos de execução \(p. 1170\)](#).

Controlar o uso dos modelos de execução

Por padrão, os usuários do IAM não têm permissões para trabalhar com modelos de execução. Você pode criar uma política de usuário do IAM que concede aos usuários permissões para criar, modificar, descrever e excluir modelos de execução e versões do modelo de execução. Você também pode aplicar permissões no nível do recurso a algumas ações do modelo de execução para controlar a capacidade de um usuário de usar recursos específicos nessas ações. Para obter mais informações, consulte as seguintes políticas de exemplo: [Exemplo: trabalhar com modelos de execução \(p. 1182\)](#).

Tenha cuidado ao conceder aos usuários permissões para usar as ações `ec2:CreateLaunchTemplate` e `ec2:CreateLaunchTemplateVersion`. Não é possível usar permissões em nível de recurso para controlar quais recursos os usuários podem especificar no modelo de execução. Para restringir os recursos usados para executar uma instância, conceda permissões para criar modelos de execução e versões de modelo de execução somente a administradores apropriados.

Criar um modelo de execução

Crie um novo modelo de execução usando parâmetros definidos por você ou use um modelo de execução ou uma instância existente como a base para o novo modelo de execução.

Tarefas

- [Criar um novo modelo de execução usando parâmetros definidos \(p. 427\)](#)
- [Criar um modelo de execução a partir de um modelo de execução existente \(p. 432\)](#)
- [Criar um modelo de execução a partir de uma instância \(p. 432\)](#)

Criar um novo modelo de execução usando parâmetros definidos

Console

Como criar um modelo de execução usando parâmetros definidos (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.
4. Em Template version description (Descrição da versão do modelo), forneça uma descrição breve da versão do modelo de execução.
5. Para marcar o modelo de execução na criação, expanda Template tags (Tags modelo), escolha Add Tag (Adicionar tag) e insira um par de chave e valor de tag.
6. Em Launch template contents (Conteúdo do modelo de execução), forneça as seguintes informações:
 - AMI: uma AMI na qual executar a instância. Para pesquisar todas as AMIs disponíveis, escolha Search for AMI (Pesquisar AMI). Para selecionar uma AMI usada normalmente, escolha Quick Start (Início rápido). Ou escolha AWS Marketplace ou Community AMIs (AMIs da comunidade). Você pode usar uma AMI que possui ou [encontrar uma AMI adequada](#).
 - Instance type (Tipo de instância): verifique se o tipo de instância é compatível com a AMI especificada. Para obter mais informações, consulte [Tipos de instância \(p. 149\)](#).
 - Key pair name (Nome do par de chaves): o par de chaves para a instância. Para obter mais informações, consulte [Pares de chaves do Amazon EC2 e instâncias do Windows \(p. 1209\)](#).
 - Network platform (Plataforma de rede): se a instância deve ser executada em uma VPC ou no EC2-Classic, se aplicável. Se você escolher VPC, especifique a sub-rede na seção Network interfaces (Interfaces de rede). Se escolher Classic, verifique se o tipo de instância especificado é compatível com o EC2-Classic e especifique a zona de disponibilidade da instância.
 - Security groups (Grupos de segurança): um ou mais grupos de segurança a serem associados à instância. Se você adicionar uma interface de rede ao modelo de execução, omita essa configuração e especifique os grupos de segurança como parte da especificação da interface de rede. Não é possível executar uma instância a partir de um modelo de inicialização que especifique grupos de segurança e uma interface de rede. Para obter mais informações, consulte [Grupos de segurança do Amazon EC2 para instâncias do Windows \(p. 1217\)](#).
7. Em Storage (Volumes) - Armazenamento (Volumes), especifique os volumes a serem anexados à instância, além dos volumes especificados pela AMI (Volume 1 (Raiz da AMI)). Para adicionar um novo volume, escolha Add new volume (Adicionar novo volume).
 - Volume type (Tipo de volume): o armazenamento de instâncias ou os volumes do Amazon EBS aos quais associar a instância. O tipo de volume depende do tipo de instância escolhido. Para obter mais informações, consulte [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#) e [Volumes do Amazon EBS \(p. 1245\)](#).
 - Device name (Nome do dispositivo): um nome de dispositivo para o volume.
 - Snapshot: o ID do snapshot a partir do qual criar o volume.
 - Size (Tamanho): para volumes do Amazon EBS, o tamanho do armazenamento.
 - Volume type (Tipo de volume): para volumes do Amazon EBS, este é o tipo de volume. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#).
 - IOPS: para o tipo de volume Provisioned IOPS SSD, o número de operações de E/S por segundo (IOPS) ao qual o volume oferece suporte.
 - Delete on termination (Excluir no encerramento): em volumes do Amazon EBS, se excluir o volume quando a instância for encerrada. Para obter mais informações, consulte [Preservar volumes do Amazon EBS no encerramento da instância \(p. 478\)](#).
 - Encrypted (Criptografado): se o tipo de instância oferecer suporte à criptografia do EBS, você poderá habilitar a criptografia para o volume. Se você tiver habilitado a criptografia por padrão nessa região, a criptografia estará habilitada para você. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).
 - Key (Chave): a chave gerenciada pelo cliente a ser usada para a criptografia do EBS. Você poderá especificar o ARN de qualquer chave gerenciada pelo cliente criada com a chave

gerenciada pelo cliente. Se você especificar uma chave gerenciada pelo cliente, também deverá usar o Encrypted (Criptografado) para habilitar a criptografia.

8. Em Tags de recurso, especifique as [tags \(p. 1554\)](#) fornecendo combinações de chave e valor. É possível marcar a instância, os volumes, as solicitações de instância spot ou os três.
9. Em Network interfaces (Interfaces de rede), você pode especificar até duas [interfaces de rede \(p. 1002\)](#) para a instância.
 - Device index (Índice do dispositivo): o número do dispositivo da interface de rede, por exemplo, eth0 para a interface de rede principal. Se você deixar o campo em branco, a AWS criará a interface de rede principal.
 - Network interface (Interface de rede): o ID da interface de rede, ou deixe o campo em branco para que a AWS crie uma nova interface de rede.
 - Description (Descrição): (opcional) uma descrição da nova interface de rede.
 - Subnet (Sub-rede): a sub-rede na qual criar uma nova interface de rede. Para a interface de rede principal (eth0), essa é a sub-rede na qual a instância será executada. Se você tiver inserido uma interface de rede existente para eth0, a instância será executada na sub-rede na qual a interface de rede está localizada.
 - Auto-assign public IP (Atribuir IP público automaticamente): se um endereço IP público deve ser atribuído automaticamente à interface de rede com o índice de dispositivo de eth0. Essa configuração só pode ser habilitada para uma nova interface de rede.
 - Primary IP (IP principal): um endereço IPv4 privado no intervalo de sua sub-rede. Deixe em branco para permitir que a AWS escolha um endereço IPv4 privado para você.
 - Secondary IP (IP secundário): um endereço IPv4 secundário privado no intervalo de sua sub-rede. Deixe em branco para permitir que a AWS escolha um para você.
 - (Somente para IPv6) IPv6 IPs (IPs IPv6): um endereço IPv6 no intervalo da sub-rede.
 - Grupos de segurança: um ou mais grupos de segurança na VPC aos quais associar a interface de rede.
 - Delete on termination (Excluir no encerramento): se a interface de rede deve ser excluída quando a instância for excluída.
 - Índice da placa de rede: O índice da placa de rede. A interface de rede primária deve ser atribuída ao índice 0 da placa de rede. Alguns tipos de instância suportam várias placas de rede.
10. Em Advanced details (Detalhes avançados), expanda a seção para exibir os campos e especifique quaisquer parâmetros adicionais para a instância.
 - Purchasing option (Opção de compra): o modelo de compra. Escolha Request Spot instances (Solicitar instâncias spot) para solicitar ao preço spot, limitado ao preço sob demanda e escolha Customize (Personalizar) para alterar as configurações padrão da instância spot. Se você não solicitar uma instância spot, o EC2 executará uma instância sob demanda por padrão. Para obter mais informações, consulte [Spot Instances \(p. 299\)](#).
 - IAM instance profile (Perfil de instância do IAM): um perfil de instância do AWS Identity and Access Management (IAM) a ser associado à instância. Para obter mais informações, consulte [Funções do IAM para Amazon EC2 \(p. 1195\)](#).
 - Comportamento de desligamento: se a instância deve ser interrompida ou encerrada quando desligada. Para obter mais informações, consulte [Alterar o comportamento de desligamento iniciado da instância \(p. 477\)](#).
 - Stop - Hibernate behavior (Interromper - comportamento de hibernação): se a instância está habilitada para hibernação. Esse campo só é válido para instâncias que atendem aos pré-requisitos de hibernação. Para obter mais informações, consulte [Hibernar a instância do Linux sob demanda ou reservada \(p. 459\)](#).
 - Termination protection (Proteção contra encerramento): se encerramento accidental deve ser impedido. Para obter mais informações, consulte [Habilitar a proteção contra encerramento \(p. 476\)](#).

- Detailed CloudWatch monitoring (Monitoramento detalhado de CloudWatch): se o monitoramento detalhado da instância deve ser habilitado usando o Amazon CloudWatch. Aplicam-se cobranças adicionais. Para obter mais informações, consulte [Monitorar instâncias usando o CloudWatch \(p. 898\)](#).
- GPU elástica: uma aceleradora do Elastic Graphics a ser anexada à instância. Nem todos os tipos de instância são compatíveis com o Elastic Graphics. Para obter mais informações, consulte [Amazon Elastic Graphics \(p. 850\)](#).
- Elastic inference (Inferência elástica): uma aceleradora de inferência elástica a ser anexada à instância de CPU do EC2. Para obter mais informações, consulte [Trabalhando com o Amazon Elastic Inference](#) no Guia do desenvolvedor do Amazon Elastic Inference.
- T2/T3 Unlimited (T2/T3 ilimitado): se permitir que as aplicações tenham intermitência acima da linha de base pelo tempo que for necessário. Este campo é válido somente para instâncias T2, T3 e T3a. Podem se aplicar cobranças adicionais. Para obter mais informações, consulte [Instâncias expansíveis \(p. 169\)](#).
- Placement group name (Nome do grupo de posicionamento): especifique um grupo de posicionamento no qual a instância será executada. Nem todos os tipos de instância podem ser executados em um placement group. Para obter mais informações, consulte [Grupos de posicionamento \(p. 1044\)](#).
- EBS-optimized instance (Instância otimizada para EBS): fornece capacidade dedicada adicional para E/S do Amazon EBS. Nem todos os tipos de instância são compatíveis com esse recurso e cobranças adicionais aplicáveis. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).
- Reserva de capacidade: especifique se deseja iniciar a instância em qualquer reserva de capacidade open (Open), uma reserva de capacidade específica (`Target by ID`) ou um grupo de reservas de capacidade (`Target by group`). Para especificar que uma reserva de capacidade não deve ser usada, escolha `None`. Para obter mais informações, consulte [Iniciar instâncias em uma Reserva de capacidade existente \(p. 400\)](#).
- Tenancy (Locação): escolha se a instância deve ser executada em hardware compartilhado (`Shared (Compartilhado)`), isolado, hardware dedicado (`Dedicated (Dedicado)`) ou em um Host dedicado (`Dedicated host (Host dedicado)`). Se você optar por executar a instância em um Host dedicado, poderá especificar se deseja executar a instância em um grupo de recursos de host ou poderá segmentar um Host dedicado específico. Podem se aplicar cobranças adicionais. Para obter mais informações, consulte [Dedicated Instances \(p. 383\)](#) e [Dedicated Hosts \(p. 349\)](#).
- RAM disk ID (ID do disco RAM): (Válido somente para AMIs paravirtuais (PV)) Um disco RAM para a instância. Se tiver especificado um kernel, poderá ser necessário especificar um disco de RAM específico com os drivers compatíveis.
- Kernel ID (ID do kernel): (Válido somente para AMIs paravirtuais (PV)) Um kernel para a instância.
- Configurações de licenças: é possível executar instâncias com relação à configuração de licença especificada para rastrear o uso da licença. Para obter mais informações, consulte [Criar uma configuração de licença](#) no Manual do usuário do AWS License Manager.
- Metadata accessible (Metadados acessíveis): habilitar ou desabilitar o acesso aos metadados da instância. Para obter mais informações, consulte [Usar IMDSv2 \(p. 623\)](#).
- Metadata version (Versão de metadados): se você habilitar o acesso aos metadados da instância, poderá optar por exigir o uso de Serviço de metadados da instância versão 2 ao solicitar metadados da instância. Para obter mais informações, consulte [Configurar opções de metadados da instância para novas instâncias \(p. 627\)](#).
- Limite de salto de resposta de metadados: se você habilitar metadados de instância, será possível definir o número permitido de saltos de rede para o token de metadados. Para obter mais informações, consulte [Usar IMDSv2 \(p. 623\)](#).

- User data (Dados do usuário): você pode especificar dados do usuário para configurar uma instância durante a execução ou para executar um script de configuração. Para obter mais informações, consulte [Executar comandos na instância do Windows na inicialização \(p. 614\)](#).

11. Escolha Create launch template (Criar modelo de execução).

AWS CLI

Como criar um modelo de execução usando a AWS CLI

- Use o comando [create-launch-template](#). O exemplo a seguir cria um modelo de execução que especifica o seguinte:

- Uma tag para o modelo de execução (`purpose=production`)
- O tipo de instância (`r4.4xlarge`) e a AMI (`ami-8c1be5f6`) a ser executada
- O número de núcleos (4) e os threads por núcleo (2) para um total de 8 vCPUs (4 núcleos x 2 threads)
- A sub-rede na qual a instância é executada (`subnet-7b16de0c`)

O modelo atribui um endereço IP público e um endereço IPv6 à instância e cria uma tag para a instância (`Name=webserver`).

```
aws ec2 create-launch-template \
--launch-template-name TemplateForWebServer \
--version-description WebVersion1 \
--tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
--launch-template-data file://template-data.json
```

Veja a seguir um exemplo de arquivo `template-data.json`.

```
{
    "NetworkInterfaces": [
        {
            "AssociatePublicIpAddress": true,
            "DeviceIndex": 0,
            "Ipv6AddressCount": 1,
            "SubnetId": "subnet-7b16de0c"
        },
        {
            "ImageId": "ami-8c1be5f6",
            "InstanceType": "r4.4xlarge",
            "TagSpecifications": [
                {
                    "ResourceType": "instance",
                    "Tags": [
                        {
                            "Key": "Name",
                            "Value": "webserver"
                        }
                    ]
                }
            ],
            "CpuOptions": {
                "CoreCount": 4,
                "ThreadsPerCore": 2
            }
        }
}
```

A seguir está um exemplo de saída.

```
{
    "LaunchTemplate": {
        "LatestVersionNumber": 1,
```

```
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

Criar um modelo de execução a partir de um modelo de execução existente

Para criar um modelo de execução de um modelo existente usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.
4. Em Template version description (Descrição da versão do modelo), forneça uma descrição breve da versão do modelo de execução.
5. Para marcar o modelo de execução na criação, expanda Template tags (Tags modelo), escolha Add Tag (Adicionar tag) e insira um par de chave e valor de tag.
6. Expanda o Modelo de origem e, em Nome do modelo de execução, escolha um modelo de execução no qual o novo modelo de execução se baseará.
7. Em Source template version (Versão do modelo de origem), escolha a versão do modelo de execução no qual o novo modelo de execução se baseará.
8. Ajuste todos os parâmetros de execução quando necessário e escolha Create launch template (Criar modelo de execução).

Criar um modelo de execução a partir de uma instância

Console

Como criar um modelo de execução a partir de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Create template from instance (Criar modelo a partir da instância).
4. Forneça um nome, uma descrição e tags e ajuste os parâmetros de execução conforme necessário.

Note

Quando você cria um modelo de execução de uma instância, os IDs da interface de rede da instância e os endereços IP não são incluídos no modelo.

5. Escolha Create launch template (Criar modelo de execução).

AWS CLI

É possível usar a AWS CLI para criar um modelo de execução de uma instância existente ao obter os dados do modelo de execução primeiro e depois criar um modelo de execução usando os dados dele.

Como obter dados de modelo de execução de uma instância usando a AWS CLI

- Use o comando `get-launch-template-data` e especifique o ID da instância. Você pode usar o resultado como base para criar um novo modelo de execução ou uma versão de modelo de execução. Por padrão, o resultado inclui um objeto `LaunchTemplateData` de nível superior, que não pode ser especificado nos dados do modelo de execução. Use a opção `--query` para excluir este objeto.

```
aws ec2 get-launch-template-data \
--instance-id i-0123d646e8048babc \
--query "LaunchTemplateData"
```

A seguir está um exemplo de saída.

```
{
    "Monitoring": {},
    "ImageId": "ami-8c1be5f6",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/xvda",
            "Ebs": {
                "DeleteOnTermination": true
            }
        }
    ],
    "EbsOptimized": false,
    "Placement": {
        "Tenancy": "default",
        "GroupName": "",
        "AvailabilityZone": "us-east-1a"
    },
    "InstanceType": "t2.micro",
    "NetworkInterfaces": [
        {
            "Description": "",
            "NetworkInterfaceId": "eni-35306abc",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.72"
                }
            ],
            "SubnetId": "subnet-7b16de0c",
            "Groups": [
                "sg-7c227019"
            ],
            "Ipv6Addresses": [
                {
                    "Ipv6Address": "2001:db8:1234:1a00::123"
                }
            ],
            "PrivateIpAddress": "10.0.0.72"
        }
    ]
}
```

Você pode gravar o resultado diretamente em um arquivo, por exemplo:

```
aws ec2 get-launch-template-data \
--instance-id i-0123d646e8048babc \
--query "LaunchTemplateData" >> instance-data.json
```

Para criar um modelo de execução usando dados do modelo de execução

Use o comando [create-launch-template](#) para criar um modelo de execução usando a saída do procedimento anterior. Para obter mais informações sobre como criar um modelo de execução usando a AWS CLI, consulte [Criar um novo modelo de execução usando parâmetros definidos \(p. 427\)](#).

Modificar um modelo de inicialização (gerenciar versões do modelo de inicialização)

Os modelos de inicialização são imutáveis. Após criar um modelo de inicialização, você não poderá modificá-lo. Em vez disso, é possível criar uma nova versão do modelo de inicialização que inclua as alterações necessárias.

Você pode criar versões de modelo de execução para um modelo de execução específico, definir uma versão padrão, descrever uma versão de modelo de execução e excluir as versões que não são mais necessárias.

Tarefas

- [Criar uma versão de modelo de execução \(p. 434\)](#)
- [Definir a versão do modelo de execução padrão \(p. 435\)](#)
- [Descrever uma versão de modelo de execução \(p. 435\)](#)
- [Excluir uma versão de modelo de execução \(p. 436\)](#)

Criar uma versão de modelo de execução

Ao criar uma versão de modelo de execução, você pode especificar novos parâmetros de execução ou usar uma versão existente como base para a nova versão. Para obter mais informações sobre os parâmetros de execução, consulte [Criar um modelo de execução \(p. 427\)](#).

Console

Para criar uma versão de modelo de execução usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione um modelo de execução e escolha Actions (Ações), Modify template (Create new version) (Modificar modelo (Criar versão)).
4. Em Template version description (Descrição da versão do modelo), insira uma descrição para a versão do modelo de execução.
5. (Opcional) Expanda o Source template (Modelo de origem) e selecione uma versão do modelo de execução a ser usado como base para a nova versão do modelo de execução. A nova versão de modelo de execução herdará os parâmetros de execução desta versão do modelo de execução.
6. Modifique os parâmetros de execução conforme necessário e escolha Create launch template (Criar modelo de execução).

AWS CLI

Como criar uma versão de modelo de execução usando a AWS CLI

- Use o comando [create-launch-template-version](#). Você pode especificar uma versão de origem na qual a nova versão será baseada. A nova versão herdará os parâmetros de execução desta versão, e você poderá substituí-los usando --launch-template-data. O exemplo a seguir cria uma nova versão com base na versão 1 do modelo de execução e especifica um ID de AMI diferente.

```
aws ec2 create-launch-template-version \
--launch-template-id lt-0abcd290751193123 \
--version-description WebVersion2 \
--source-version 1 \
--launch-template-data "ImageId=ami-c998b6b2"
```

Definir a versão do modelo de execução padrão

Você pode definir a versão padrão do modelo de execução. Quando você executa uma instância a partir de um modelo de execução e não especifica uma versão, a instância é executada por meio dos parâmetros da versão padrão.

Console

Para definir a versão de modelo de execução padrão usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Set default version (Definir versão padrão).
4. Em Template version (Versão do modelo), selecione o número da versão a ser definida como versão padrão e escolha Set as default version (Definir como versão padrão).

AWS CLI

Como definir a versão de modelo de execução padrão usando a AWS CLI

- Use o comando [modify-launch-template](#) e especifique a versão que deseja definir como padrão.

```
aws ec2 modify-launch-template \
--launch-template-id lt-0abcd290751193123 \
--default-version 2
```

Descrever uma versão de modelo de execução

Usando o console, você pode exibir todas as versões do modelo de execução selecionado ou obter uma lista dos modelos de execução cuja versão mais recente ou padrão corresponde a um número de versão específico. Usando o AWS CLI, você pode descrever todas as versões, versões individuais ou um intervalo de versões de um modelo de execução especificado. Você também pode descrever todas as versões mais recentes ou todas as versões padrão de todos os modelos de execução da sua conta.

Console

Como descrever uma versão de modelo de execução usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Você pode exibir uma versão de um modelo de lançamento específico ou obter uma lista dos modelos de execução cuja versão mais recente ou padrão corresponde a um número de versão específico.
 - Para exibir uma versão de um modelo de execução: selecione o modelo de execução. Na guia Versões em Versão, selecione uma versão para exibir seus detalhes.

- Para obter uma lista de todos os modelos de execução cuja versão mais recente corresponde a um número de versão específico: na barra de pesquisa, escolha Versão mais recente e selecione um número de versão.
- Para obter uma lista de todos os modelos de execução cuja versão padrão corresponde a um número de versão específico: na barra de pesquisa, escolha Versão padrão e selecione um número de versão.

AWS CLI

Como descrever uma versão de modelo de execução usando a AWS CLI

- Use o comando `delete-launch-template-versions` e especifique os números de versão. No exemplo a seguir, as versões 1 e 3 são especificadas.

```
aws ec2 describe-launch-template-versions \
--launch-template-id lt-abcd290751193123 \
--versions 1 3
```

Como descrever todas as versões mais recentes e padrão do modelo de execução na sua conta usando a AWS CLI

- Use o comando `describe-launch-template-versions` e especifique `$Latest`, `$Default`, ou ambos. Você deve omitir o ID e o nome do modelo de execução na chamada. Não é possível especificar números de versão.

```
aws ec2 describe-launch-template-versions \
--versions "$Latest,$Default"
```

Excluir uma versão de modelo de execução

Caso não precise mais de uma versão de modelo de execução, exclua-a. Não será possível substituir o número de versão após excluí-lo. Você não pode excluir a versão padrão do modelo de execução; você deve primeiro atribuir outra versão como padrão.

Console

Para excluir uma versão de modelo de execução usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Delete template version (Excluir versão de modelo).
4. Selecione a versão a ser excluída e escolha Delete (Excluir).

AWS CLI

Como excluir uma versão de modelo de execução usando a AWS CLI

- Use o comando `delete-launch-template-versions` e especifique os números de versão a serem excluídos.

```
aws ec2 delete-launch-template-versions \
--launch-template-id lt-abcd290751193123 \
```

--versions 1

Executar uma instância a partir de um modelo de execução

Você pode usar os parâmetros contidos em um modelo de execução para executar uma instância. É possível substituir ou adicionar parâmetros de execução antes de executar a instância.

As instâncias executadas por meio de um modelo de execução recebem automaticamente duas tags com as chaves `aws:ec2launchtemplate:id` e `aws:ec2launchtemplate:version`. Não é possível remover ou editar essas tags.

Console

Para executar uma instância a partir de um modelo de execução usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Launch instance from template (Executar instância do modelo).
4. Em Source template version (Versão do modelo de origem), selecione a versão do modelo de execução a ser usado.
5. Em Number of instances (Número de instâncias), especifique o número de instâncias a serem executadas.
6. (Opcional) Você pode substituir ou adicionar parâmetros de modelo de execução alterando e adicionando parâmetros na seção Instance details (Detalhes da instância).
7. Escolha Launch instance from template (Executar instância do modelo).

AWS CLI

Como executar uma instância a partir de um modelo de execução usando a AWS CLI

- Use o comando `run-instances` e especifique o parâmetro `--launch-template`. Se desejar, especifique a versão de modelo de execução a ser usada. Se você não especificar a versão, a versão padrão será usada.

```
aws ec2 run-instances \
--launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Para substituir um parâmetro de modelo de execução, especifique o parâmetro no comando `run-instances`. O exemplo a seguir substitui o tipo de instância especificado no modelo de execução (se houver algum).

```
aws ec2 run-instances \
--launch-template LaunchTemplateId=lt-0abcd290751193123 \
--instance-type t2.small
```

- Se você especificar um parâmetro aninhado que faça parte de uma estrutura complexa, a instância será executada por meio da estrutura complexa conforme especificado no modelo de execução, além de quaisquer parâmetros aninhados adicionais que você especificar.

No exemplo a seguir, a instância é executada com a tag `Owner=TeamA`, bem como com quaisquer outras tags especificadas no modelo de execução. Se o modelo de execução tiver uma tag com uma chave `Owner`, o valor será substituído por `TeamA`.

```
aws ec2 run-instances \
```

```
--launch-template LaunchTemplateId=lt-0abcd290751193123 \
--tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

No exemplo a seguir, a instância é executada com um volume com o nome de dispositivo /dev/xvdb, bem como com quaisquer outros mapeamentos de dispositivos de blocos especificados no modelo de execução. Se o modelo de execução tiver um volume existente definido para /dev/xvdb, seus valores serão substituídos pelos valores especificados.

```
aws ec2 run-instances \
--launch-template LaunchTemplateId=lt-0abcd290751193123 \
--block-device-mappings "DeviceName=/dev/xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

Se a instância não executar ou o estado passar imediatamente para terminated, em vez de running, consulte [Solucionar problemas de execução de instâncias \(p. 1570\)](#).

Usar modelos de execução com o Amazon EC2 Auto Scaling

Você pode criar um grupo do Auto Scaling e especificar um modelo de execução a ser usado no grupo. Quando o Amazon EC2 Auto Scaling executar instâncias no grupo do Auto Scaling, ele usará os parâmetros de execução definidos no modelo de execução associado. Para obter mais informações, consulte [Criação de um grupo do Auto Scaling usando um modelo de execução](#) no Guia do usuário do Amazon EC2 Auto Scaling.

Antes de criar um grupo do Auto Scaling usando um modelo de execução, você deverá criar um modelo de execução que inclua os parâmetros necessários para executar uma instância em um grupo do Auto Scaling, como o ID da AMI. O console fornece orientações para ajudá-lo a criar um modelo que possa ser usado com o Auto Scaling.

Como criar um modelo de execução para uso com o Auto Scaling usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Launch Templates (Modelos de execução) e Create launch template (Criar modelo de execução).
3. Em Device template name (Nome do modelo de dispositivo), insira um nome descritivo para o modelo.
4. Em Template version description (Descrição da versão do modelo), forneça uma descrição breve da versão do modelo de execução.
5. Em Auto Scaling guidance (Orientação do Auto Scaling), marque a caixa de seleção para que o Amazon EC2 forneça orientações para ajudá-lo a criar um modelo para uso com o Auto Scaling.
6. Modifique os parâmetros de execução conforme necessário. Como você selecionou a orientação do Auto Scaling, alguns campos são obrigatórios e alguns ficam indisponíveis. Para considerações sobre a criação de um modelo de execução e para obter informações sobre como configurar os parâmetros de execução do Auto Scaling, consulte [Criar um modelo de execução para um grupo de Auto Scaling](#) no Guia do usuário do Amazon EC2 Auto Scaling.
7. Escolha Create launch template (Criar modelo de execução).
8. (Opcional) Para criar um grupo do Auto Scaling usando esse modelo de execução, na página Next steps (Próximas etapas), escolha Create Auto Scaling group (Criar grupo do Auto Scaling).

Para criar ou atualizar um grupo do Amazon EC2 Auto Scaling com um modelo de execução usando a AWS CLI

- Use o comando `create-auto-scaling-group` ou `update-auto-scaling-group` e especifique o parâmetro `--launch-template`.

Usar modelos de execução com o Frotas do EC2

Você pode criar uma solicitação de um Frotas do EC2 e especificar um modelo de execução na configuração da instância. Quando o Amazon EC2 atender à solicitação do Frotas do EC2, ele usará os parâmetros de execução definidos no modelo de execução associado. Você pode substituir alguns parâmetros especificados no modelo de execução.

Para obter mais informações, consulte [Criar uma Frotas do EC2. \(p. 751\)](#).

Para criar uma EC2 Fleet com um modelo de execução usando a AWS CLI

- Use o comando `create-fleet`. Use o parâmetro `--launch-template-configs` para especificar o modelo de execução e quaisquer substituições para o modelo de execução.

Usar modelos de execução com a frota spot

Você pode criar uma solicitação de uma frota spot e especificar um modelo de execução na configuração da instância. Quando o Amazon EC2 atender à solicitação da frota spot, ele usará os parâmetros de execução definidos no modelo de execução associado. Você pode substituir alguns parâmetros especificados no modelo de execução.

Para obter mais informações, consulte [Tipos de solicitação da frota spot \(p. 761\)](#).

Para criar uma solicitação de frota spot com um modelo de execução usando a AWS CLI

- Use o comando `request-spot-fleet`. Use o parâmetro `LaunchTemplateConfigs` para especificar o modelo de execução e quaisquer substituições para o modelo de execução.

Excluir um modelo de execução

Caso não precise mais de um modelo de execução, exclua-o. A exclusão de um modelo de execução excluirá todas as suas versões.

Console

Para excluir um modelo de execução (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Launch Templates (Modelos de execução).
3. Selecione o modelo de execução e escolha Actions (Ações), Delete template (Excluir modelo).
4. Digite **Delete** para confirmar a exclusão e escolha Delete (Excluir).

AWS CLI

Para excluir um modelo de execução (AWS CLI)

- Use o comando `delete-launch-template` (AWS CLI) e especifique o modelo de execução.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

Executar uma instância usando parâmetros de uma instância existente

O console do Amazon EC2 fornece uma opção de assistente Launch more like this (Executar mais como esta) que permite a você usar uma instância atual como base para a execução de outras instâncias. Essa opção preenche automaticamente o assistente de execução do Amazon EC2 com determinados detalhes de configuração da instância selecionada.

Note

A opção do assistente Launch more like this (Executar mais como esta) não clona sua instância selecionada; somente replica alguns detalhes de configuração. Para criar uma cópia da sua instância, primeiro crie uma AMI a partir dela e então execute mais instâncias a partir da AMI. Se desejar, crie um [modelo de execução \(p. 425\)](#) para armazenar os parâmetros de execução das instâncias.

Os detalhes de configuração a seguir são copiados da instância selecionada para o assistente de execução:

- ID de AMI
- Tipo de instância
- Zona de disponibilidade, ou a VPC e a sub-rede nas quais a instância selecionada fica localizada
- Endereço IPv4 público. Se a instância selecionada atualmente tiver um endereço IPv4 público, a nova instância receberá um endereço IPv4 público – independentemente da configuração do endereço IPv4 público padrão da instância selecionada. Para mais informações sobre endereços IPv4 públicos, consulte [Endereços IPv4 públicos e nomes de host DNS externos \(p. 957\)](#).
- Grupo de posicionamento, se aplicável
- A função do IAM associada à instância, se aplicável
- Configuração de comportamento de desativação (interromper ou encerrar)
- Configuração de proteção de encerramento (verdadeiro ou falso)
- Monitoramento do CloudWatch (habilitado ou desabilitado)
- Configuração de otimização do Amazon EBS (verdadeiro ou falso)
- Configuração de locação, se executando dentro de uma VPC (compartilhada ou dedicada)
- ID do kernel e ID do disco RAM, se aplicável
- Dados do usuário, se especificado
- Tags associadas à instância, se aplicável
- Security groups associados à instância
- Informações de associação. Se a instância selecionada estiver associada a um arquivo de configuração, o mesmo arquivo será automaticamente associado à nova instância. Se o arquivo de configuração incluir uma configuração de domínio ingressado, a nova instância será ingressada no mesmo domínio. Para obter mais informações sobre como ingressar em um domínio, consulte [Seamlessly Join a Windows EC2 Instance \(Associe continuamente uma instância do EC2 do Windows\)](#) no AWS Directory Service Administration Guide (Guia de administração do AWS Directory Service).

Os seguintes detalhes da configuração não são copiados da instância selecionada. Em vez disso, o assistente aplica as configurações ou o comportamento padrão:

- Número de interfaces de rede: O padrão é uma interface de rede, que é a interface de rede primária (eth0).
- Armazenamento: A configuração de armazenamento padrão é determinada pela AMI e pelo tipo de instância.

New console

Para usar a instância atual como modelo

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que deseja usar e escolha Actions (Ações), Images and templates (Imagens e modelos) e Launch more like this (Executar mais como esta).
4. O assistente de execução abre na página Review Instance Launch (Revisar execução da instância). É possível fazer as alterações necessárias escolhendo o link Edit (Editar) apropriado.

Quando estiver pronto, escolha Launch (Executar) para selecionar um par de chaves e execute sua instância.

5. Se a instância não executar ou o estado passar imediatamente para terminated, em vez de running, consulte [Solucionar problemas de execução de instâncias \(p. 1570\)](#).

Old console

Para usar a instância atual como modelo

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que deseja usar e escolha Actions (Ações), Launch more like this (Executar mais como esta).
4. O assistente de execução abre na página Review Instance Launch (Revisar execução da instância). É possível fazer as alterações necessárias escolhendo o link Edit (Editar) apropriado.

Quando estiver pronto, escolha Launch (Executar) para selecionar um par de chaves e execute sua instância.

5. Se a instância não executar ou o estado passar imediatamente para terminated, em vez de running, consulte [Solucionar problemas de execução de instâncias \(p. 1570\)](#).

Executar uma instância AWS Marketplace

Você pode se inscrever em um produto da AWS Marketplace e executar uma instância a partir da AMI do produto usando o Launch Wizard do Amazon EC2. Para obter mais informações sobre AMIs pagas, consulte [AMIs pagas \(p. 115\)](#). Para cancelar sua assinatura depois do lançamento, primeiro encerre todas as instâncias sendo executadas a partir delas. Para obter mais informações, consulte [Gerenciar suas assinaturas do AWS Marketplace \(p. 119\)](#).

Para executar uma instância no AWS Marketplace usando o assistente de execução

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel do Amazon EC2, escolha Launch Instance (Executar instância).
3. Na página Choose an Amazon Machine Image (AMI) (Escolher uma imagem de máquina da Amazon), escolha a categoria AWS Marketplace à esquerda. Encontre uma AMI adequada navegando pelas categorias ou utilizando a funcionalidade de pesquisa. Escolha Select (Selecionar) para escolher seu produto.
4. A caixa de diálogo exibe uma visão geral do produto selecionado. Você pode visualizar as informações de preços, bem como quaisquer outras informações que o fornecedor fornecer. Quando você estiver pronto, escolha Continue (Continuar).

Note

Não será cobrado o uso do produto até que você execute uma instância com a AMI. Anote o preço de cada tipo de instância compatível, pois você deverá selecionar um tipo de instância na próxima página do assistente. Podem ser aplicados também impostos adicionais ao produto.

5. Na página Choose an Instance Type (Escolher um tipo de instância), selecione a configuração do hardware e o tamanho da instância a ser executada. Ao terminar, selecione Next: Configure Instance Details (Próximo: Configurar detalhes da instância).
6. Nas próximas páginas do assistente, você pode configurar a instância, adicionar armazenamento e tags. Para obter mais informações sobre as diferentes opções que você pode configurar, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#). Escolha Próximo até alcançar a página Configure Security Group .

O assistente cria um novo security group de acordo com as especificações do fornecedor do produto. O security group pode incluir regras que permitem a todos os endereços IPv4 (0.0.0.0/0) acesso a SSH (porta 22) no Linux ou RDP (porta 3389) no Windows. Recomendamos que você ajuste essas regras para permitir somente que um endereço específico ou um intervalo de endereços accessem sua instância nessas portas.

Quando estiver pronto, selecione Review and Launch (Revisar e executar).

7. Na página Review Instance Launch (Revisar execução da instância), verifique os detalhes da AMI a partir da qual você está prestes a executar a instância, assim como outros detalhes de configuração definidos no assistente. Quando você estiver pronto, escolha Launch (Executar) para selecionar ou criar um par de chaves e execute sua instância.
8. Dependendo do produto ao qual você se inscreveu, a instância pode levar alguns minutos ou mais para ser executada. Você primeiro é inscrito no produto antes de sua instância ser executada. Se houver algum problema com os detalhes do cartão de crédito, você será convidado a atualizar os detalhes da conta. Quando a página de confirmação da execução for exibida, selecione View Instances (Exibir instâncias) para acessar a página Instâncias.

Note

De você será cobrado o preço da assinatura, desde que sua instância esteja em execução, mesmo se estiver inativa. Se sua instância for interrompida, você ainda pode ser cobrado pelo armazenamento.

9. Quando o status da sua instância estiver no estado `running`, você poderá se conectar a ela. Para fazer isso, selecione sua instância na lista e escolha Connect (Conectar). Siga as instruções na caixa de diálogo. Para obter mais informações sobre como se conectar à sua instância, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).

Important

Verifique as instruções de uso do fornecedor com cuidado, pois você pode precisar usar um nome de usuário específico para efetuar login na instância. Para obter mais informações sobre como acessar os detalhes de assinatura, consulte [Gerenciar suas assinaturas do AWS Marketplace \(p. 119\)](#).

10. Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte [Solucionar problemas de execução de instâncias \(p. 1570\)](#).

Executar uma instância de AMI de AWS Marketplace usando a API e a CLI

Para executar instâncias de produtos do AWS Marketplace usando a API ou as ferramentas de linha de comando, primeiro garanta que você esteja inscrito no produto. Você pode então executar uma instância com o ID da AMI do produto usando os seguintes métodos:

Método	Documentação
AWS CLI	Use o comando run-instances ou consulte o tópico a seguir para obter mais informações: Execução de uma instância .
AWS Tools for Windows PowerShell	Use o comando New-EC2Instance ou consulte o tópico a seguir para obter mais informações: Executar uma instância do Amazon EC2 usando o Windows PowerShell
API de consulta	Use a solicitação RunInstances .

Conectar-se à sua instância do Windows

É possível se conectar às instâncias do Amazon EC2 criadas da maioria das imagens de máquina da Amazon (AMIs) usando o Desktop Remoto. O Remote Desktop usa o [Remote Desktop Protocol \(RDP\)](#) para conectar e usar sua instância da mesma forma que você usa um computador que esteja na sua frente (computador local). Ele está disponível na maioria das edições do Windows e também para Mac OS.

A licença do sistema operacional (SO) Windows Server permite duas conexões remotas simultâneas para fins administrativos. A licença para Windows Server está incluída no preço da sua instância do Windows. Caso precise de mais de duas conexões remotas simultâneas, você deverá adquirir uma licença do Remote Desktop Services (RDS). Se você tentar uma terceira conexão, ocorrerá um erro.

Para obter informações sobre como se conectar a uma instância Linux, consulte [Conectar-se à sua instância do Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

- [Prerequisites \(p. 443\)](#)
- [Conectar-se à sua instância baseada no Windows usando RDP \(p. 444\)](#)
- [Conectar-se a uma instância do Windows usando seu endereço IPv6 \(p. 450\)](#)
- [Conectar-se a uma instância do Windows usando o Session Manager \(p. 452\)](#)
- [Configurar suas contas \(p. 453\)](#)
- [Transferir arquivos para instâncias do Windows \(p. 453\)](#)

Prerequisites

- Instalação de um cliente RDP
 - [Windows] O Windows inclui um cliente RDP por padrão. Para verificar, digite mstsc em uma janela de Prompt de Comando. Se o computador não reconhecer esse comando, consulte a [página inicial do Windows](#) e pesquise pelo download da aplicação do Desktop Remoto da Microsoft.
 - [Mac OS X] Faça download da [aplicação Microsoft Remote Desktop](#) na Mac App Store.
 - [Linux] Use [Remmina](#).
- Encontrar a chave privada

Obtenha o caminho totalmente qualificado para o local em seu computador do arquivo .pem para o par de chaves que você especificou quando executou a instância. Para obter mais informações, consulte [Identificar o par de chaves que foi especificado ao iniciar](#). Se você não conseguir encontrar seu arquivo de chave privada, consulte [Conectar-se à instância do Windows em caso de perda da chave privada](#).

- Permitir tráfego RDP de entrada do endereço IP à instância

Verifique se o grupo de segurança associado à instância permite tráfego RDP de entrada (port 3389) do endereço IP. O grupo de segurança padrão não permite o tráfego RDP de entrada. Para obter mais informações, consulte [Autorizar tráfego de entrada para suas instâncias do Windows \(p. 1205\)](#).

Conectar-se à sua instância baseada no Windows usando RDP

Para se conectar a uma instância Windows, você deve recuperar a senha do administrador e inserir essa senha ao se conectar à sua instância usando o Desktop Remoto. Após a execução da instância, leva alguns minutos para que a senha fique disponível.

O nome da conta de administrador depende do idioma do sistema operacional. Por exemplo, em inglês é **Administrator**, em francês é **Administrateur** e em português é **Administrador**. Para obter mais informações, consulte [Localized Names for Administrator Account in Windows \(Nomes localizados da conta de administrador no Windows\)](#) no Microsoft TechNet Wiki.

Se você associou sua instância a um domínio, poderá se conectar a sua instância usando credenciais de domínio definidas no AWS Directory Service. Na tela de logon do Desktop Remoto, em vez de usar o nome do computador local e a senha gerada, use o nome de usuário totalmente qualificado para o administrador (por exemplo, **corp.example.com\Admin**) e a senha dessa conta.

Se você receber um erro ao tentar se conectar à instância, consulte [O Remote Desktop não pode se conectar ao computador remoto \(p. 1574\)](#).

New console

Para se conectar à sua instância do Windows usando um cliente RDP

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instances (Instâncias). Selecione a instância e escolha Conectar.
3. Na página Connect to instance (Conectar à instância), escolha a guia RDP client (Cliente RDP) e depois Get password (Obter senha).

Connect to instance [Info](#)
Connect to your instance i-██████████ using any of these options

Session Manager **RDP client** EC2 Serial Console

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

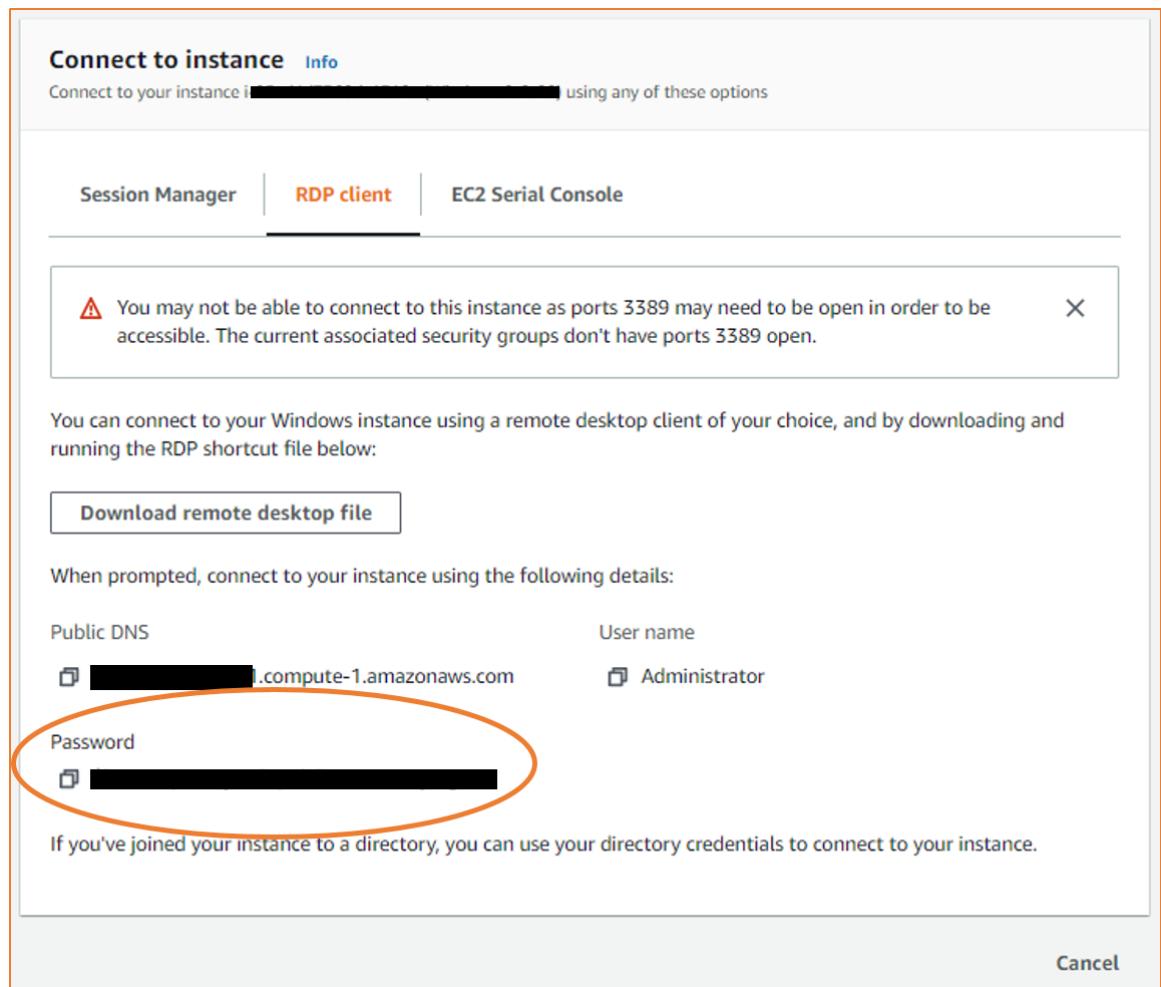
When prompted, connect to your instance using the following details:

Public DNS	User name
<input type="text"/> ec2-100-25-146-1.compute-1.amazonaws.com	<input type="text"/> Administrator
Password	Get password

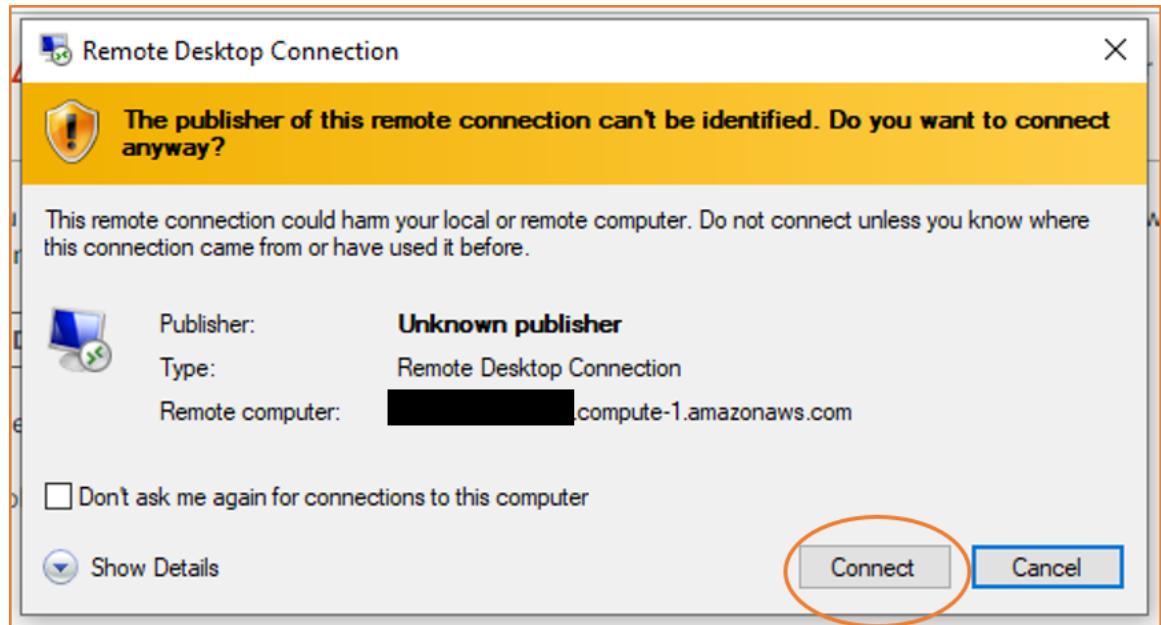
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

[Cancel](#)

4. Escolha Browse (Navegar) e navegue até o arquivo de chave privada (.pem) que você criou ao iniciar a instância. Selecione o arquivo e escolha Open (Abrir) para copiar todo o conteúdo do arquivo para essa janela.
5. Escolha Decrypt Password. O console exibe a senha de administrador padrão correspondente à instância em Password (Senha), substituindo o link Get Password (Obter senha) exibido anteriormente. Salve a senha em um lugar seguro. Essa senha é necessária para se conectar à instância.



6. Escolha Download remote desktop file (Fazer download de arquivo do desktop remoto). O navegador pergunta se você quer abrir ou salvar o arquivo de atalho RDP. Quando terminar o download do arquivo, escolha Cancel (Cancelar) para retornar à página Instances (Instâncias).
 - Se tiver aberto o arquivo RDP, você verá a caixa de diálogo Remote Desktop Connection (Conexão de Desktop Remoto).
 - Se você tiver salvado o arquivo RDP, navegue até o diretório de downloads e abra o arquivo RDP para exibir a caixa de diálogo.
7. Talvez você receba um aviso de que o publicador da conexão remota é desconhecido. Escolha Connect (Conectar) para se conectar à sua instância.

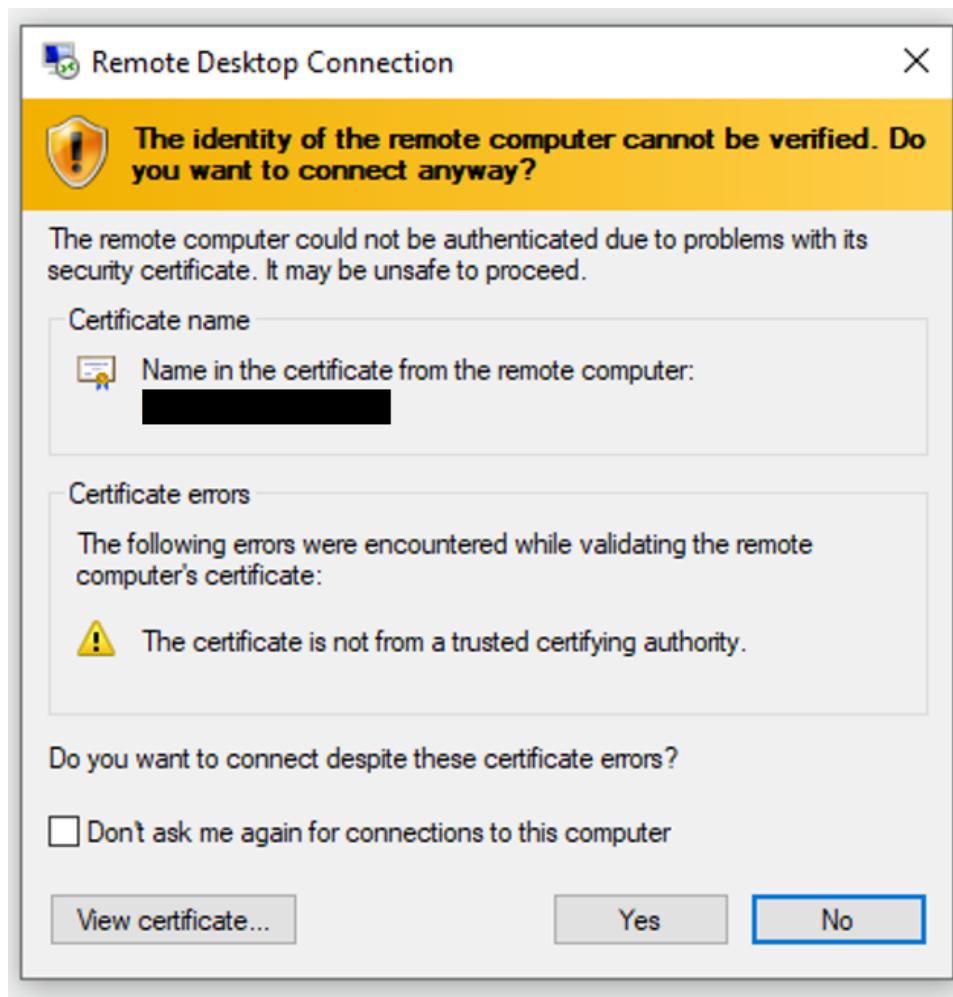


8. A conta de administrador é escolhida por padrão. Copie e cole a senha que você salvou anteriormente.

Tip

Se você receber o erro “Password Failed” (Senha incorreta), tente digitar a senha manualmente. As senhas podem ser corrompidas ao copiar e colar.

9. Devido à natureza dos certificados autoassinados, talvez você receba um aviso indicando que o certificado de segurança não pode ser autenticado. Siga as etapas abaixo para confirmar a identidade do computador remoto ou apenas escolha Yes (Sim) (Windows) ou Continue (Continuar) (Mac OS X) caso confie no certificado.



- a. Se estiver usando a Remote Desktop Connection (Conexão de Desktop Remoto) em um computador Windows, escolha View certificate (Exibir certificado). Se estiver usando o Microsoft Remote Desktop em um Mac, escolha Show Certificate.
- b. Selecione a guia Details (Detalhes) e role para baixo até Thumbprint (Impressão digital) (Windows) ou SHA1 Fingerprints (Impressões digitais SHA1) (Mac OS X). Esse é o identificador exclusivo do certificado de segurança do computador remoto.
- c. No console do Amazon EC2, selecione a instância, escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema).
- d. Procure por RDPCERTIFICATE-THUMBPRINT na saída do log: Se esse valor corresponder à impressão digital do certificado, você terá verificado a identidade do computador remoto.
- e. Se estiver usando a Remote Desktop Connection (Conexão de Desktop Remoto) em um computador Windows, volte à caixa de diálogo Certificate (Certificado) e escolha OK. Se estiver usando o Microsoft Remote Desktop em um Mac, volte para Verify Certificate e escolha Continue.
- f. [Windows] Escolha Yes (Sim) na janela Remote Desktop Connection (Conexão de Desktop Remoto) para se conectar à instância.

[Mac OS X] Faça login conforme solicitado, usando a conta de administrador padrão e a senha de administrador padrão que você registrou ou copiou anteriormente. Observe que pode ser necessário alternar espaços para ver a tela de login. Para obter mais informações, consulte [Add spaces and switch between them](#) (Adicionar espaços e alternar entre eles).

Old console

Para se conectar à sua instância do Windows usando um cliente RDP

1. No console do Amazon EC2, selecione a instância e, em seguida, escolha Connect (Conectar-se).
2. Na caixa de diálogo Connect To Your Instance, escolha Get Password (depois que a instância é lançada, demora alguns minutos para que a senha fique disponível).
3. Escolha Browse (Navegar) e navegue até o arquivo de chave privada (.pem) que você criou ao iniciar a instância. Selecione o arquivo e escolha Open para copiar todo o conteúdo do arquivo para o campo Contents.
4. Escolha Decrypt Password. O console exibe a senha de administrador padrão correspondente à instância na caixa de diálogo Connect To Your Instance, substituindo o link para Get Password mostrado anteriormente pela senha real.
5. Registre a senha de administrador padrão ou copie-para a área de transferência. Você precisará dessa senha para se conectar à instância.
6. Escolha Download Remote Desktop File. O navegador pergunta se você quer abrir ou salvar o arquivo .rdp. Qualquer uma das opções é aceitável. Quando terminar, você poderá escolher Close para descartar a caixa de diálogo Connect To Your Instance.
 - Se tiver aberto o arquivo .rdp, você verá a caixa de diálogo Remote Desktop Connection (Conexão de Desktop Remoto).
 - Se você tiver salvado o arquivo .rdp, navegue até o diretório de downloads e abra o arquivo .rdp para exibir a caixa de diálogo.
7. Talvez você receba um aviso de que o publicador da conexão remota é desconhecido. Você pode continuar se conectando à instância.
8. Quando solicitado, faça login na instância usando a conta do administrador do sistema operacional e a senha registrada ou copiada por você anteriormente. Caso sua Remote Desktop Connection (Conexão de Desktop Remoto) já tenha uma conta de administrador configurada, talvez seja necessário escolher a opção Use another account (Usar outra conta) e digitar o nome de usuário e senha manualmente.

Note

Às vezes, quando se copia e cola conteúdo, os dados podem ser corrompidos. Se você encontrar o erro "Password Failed" ao fazer login, experimente digitar a senha manualmente.

9. Devido à natureza dos certificados autoassinados, talvez você receba um aviso indicando que o certificado de segurança não pôde ser autenticado. Siga as etapas abaixo para confirmar a identidade do computador remoto ou apenas escolha Yes ou Continue para continuar, caso confie no certificado.
 - a. Se estiver usando a Conexão de Desktop Remoto em um PC Windows, escolha View certificate. Se estiver usando o Microsoft Remote Desktop em um Mac, escolha Show Certificate.
 - b. Escolha a guia Details (Detalhes) e role a tela para baixo até a entrada Thumbprint (Impressão digital) em um PC com o Windows ou a entrada SHA1 Fingerprints (Impressões digitais com SHA1) em um Mac. Esse é o identificador exclusivo do certificado de segurança do computador remoto.
 - c. No console do Amazon EC2, selecione a instância, escolha Actions (Ações) e, em seguida, escolha Get System Log (Obter log do sistema).
 - d. Na saída do log do sistema, procure uma entrada rotulada RDPCERTIFICATE-THUMBPRINT. Se esse valor corresponder à impressão digital do certificado, você terá verificado a identidade do computador remoto.

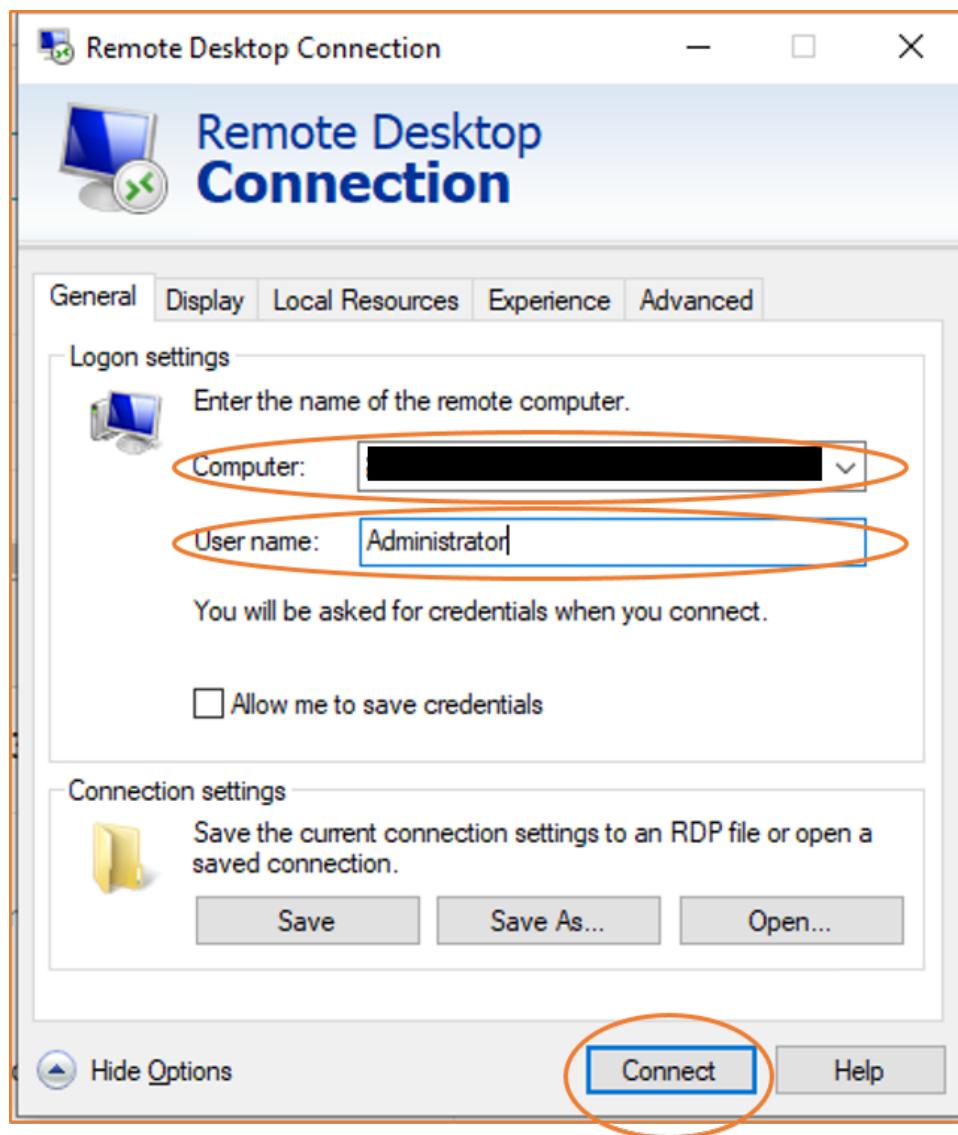
- e. Se estiver usando a Conexão de Desktop Remoto em um PC Windows, volte à caixa de diálogo Certificate e escolha OK. Se estiver usando o Microsoft Remote Desktop em um Mac, volte para Verify Certificate e escolha Continue.
- f. [Windows] Escolha Yes na janela Remote Desktop Connection para se conectar à instância.
[Mac OS] Faça login conforme solicitado, usando a conta de administrador padrão e a senha de administrador padrão que você registrou ou copiou anteriormente. Observe que pode ser necessário alternar espaços para ver a tela de login. Para mais informações sobre espaços, consulte support.apple.com/pt-br/HT204100.
- g. Se você receber um erro ao tentar se conectar à instância, consulte [O Remote Desktop não pode se conectar ao computador remoto \(p. 1574\)](#).

Conectar-se a uma instância do Windows usando seu endereço IPv6

Se você [habilitou a VPC para IPv6 e atribuiu um endereço IPv6 à sua instância Windows \(p. 963\)](#), poderá usar um cliente RDP para se conectar à sua instância usando seu endereço IPv6 (por exemplo, 2001:db8:1234:1a00:9691:9503:25ad:1761) em vez de um endereço IPv4 público ou nome de host DNS público.

Para conectar-se à sua instância do Windows usando seu endereço IPv6

1. Obtenha a senha inicial de administrador para sua instância, conforme descrito em [Conectar-se à sua instância baseada no Windows usando RDP \(p. 444\)](#). Essa senha é necessária para se conectar à sua instância.
2. [Windows] Abra o cliente RDP em um computador Windows, escolha Show Options (Mostrar opções) e faça o seguinte:



- Em Computer (Computador), insira o endereço IPv6 da instância do Windows.
- Em User name (Nome do usuário), digite Administrator (Administrador).
- Selecione Conectar.
- Quando solicitado, digite a senha que você salvou anteriormente.

[Mac OS X] Abra o cliente RDP no computador e faça o seguinte:

- Escolha Novo.
 - Em PC Name (Nome do PC), digite o endereço IPv6 da instância do Windows.
 - Em User name (Nome do usuário), digite Administrator (Administrador).
 - Feche a caixa de diálogo. Em My Desktops (Meus desktops), selecione a conexão e escolha Start (Iniciar).
 - Quando solicitado, digite a senha que você salvou anteriormente.
3. Devido à natureza dos certificados autoassinados, talvez você receba um aviso indicando que o certificado de segurança não pode ser autenticado. Se você confia no certificado, pode

escolher Yes (Sim) ou Continue (Continuar). Caso contrário, você pode verificar a identidade do computador remoto, conforme descrito em [Conectar-se à sua instância baseada no Windows usando RDP \(p. 444\)](#).

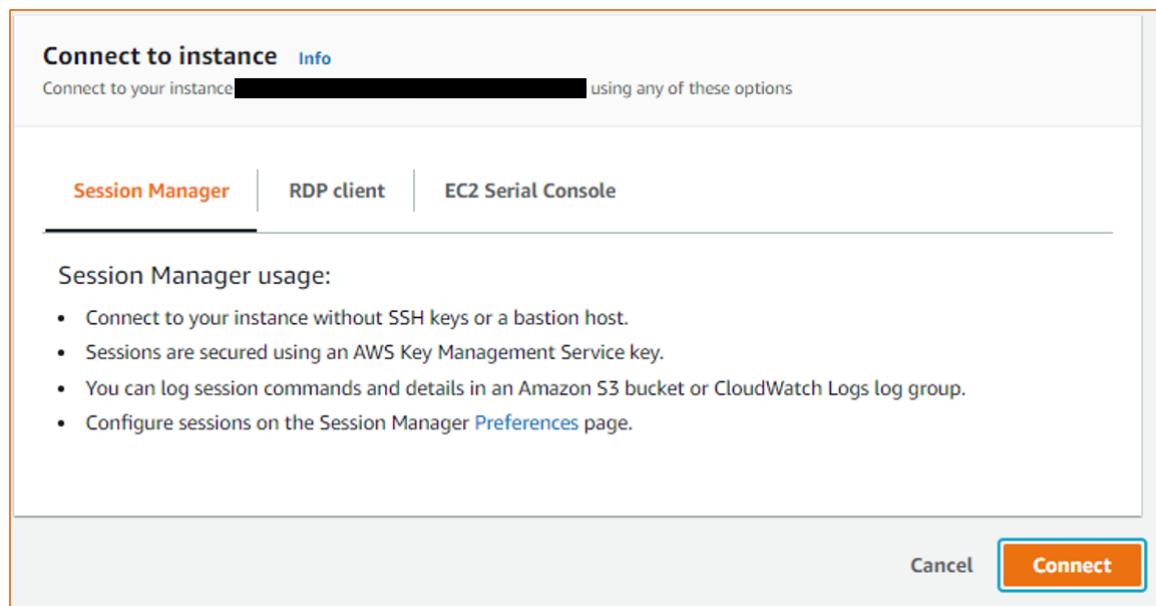
Conectar-se a uma instância do Windows usando o Session Manager

O Session Manager é um recurso totalmente gerenciado do AWS Systems Manager para gerenciar suas instâncias do Amazon EC2 por meio de um shell interativo baseado no navegador com um clique ou por meio da AWS CLI. Você pode usar o Gerenciador de sessões para iniciar uma sessão com uma instância na sua conta. Depois que a sessão é iniciada, você pode executar comandos do PowerShell da mesma forma como faria para qualquer outro tipo de conexão. Para obter mais informações sobre o Gerenciador de sessões, consulte [Gerenciador de sessões do AWS Systems Manager](#) no Guia do usuário do AWS Systems Manager.

Antes de tentar se conectar a uma instância usando o Gerenciador de sessões, verifique se as etapas de configuração necessárias foram concluídas. Para obter mais informações, consulte [Conceitos básicos do Gerenciador de sessões](#).

Como se conectar a uma instância do Windows usando o Session Manager no console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Connect (Conectar).
4. Em Connection method (Método de conexão), escolha Session Manager (Gerenciador de sessões).
5. Selecione Conectar.



Tip

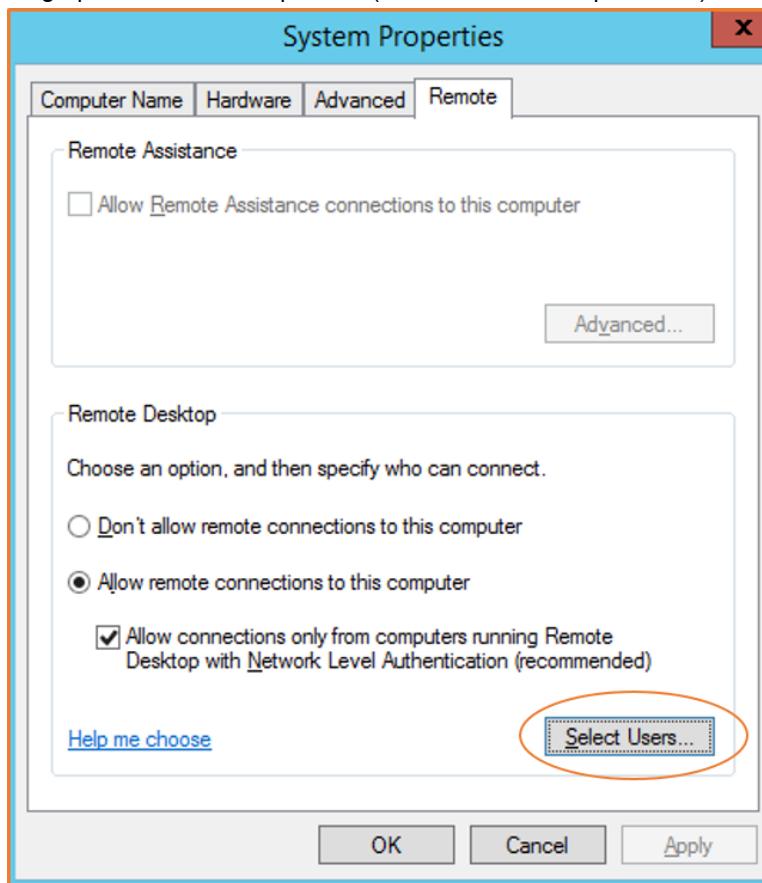
Se você receber um erro informando que não tem autorização para executar uma ou mais ações do Systems Manager (`ssm:command-name`), será necessário atualizar suas políticas para permitir que inicie sessões pelo console do Amazon EC2. Para obter mais informações e instruções, consulte [Quickstart Default IAM Policies for Session Manager](#)

(Políticas padrão do IAM do Quickstart para Session Manager) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

Configurar suas contas

Após se conectar, recomendamos efetuar o seguinte:

- Altere a senha de administrador do valor padrão. Você [pode alterar a senha enquanto estiver conectado à instância](#), assim como faria em qualquer outro computador executando o Windows Server.
- Crie outra conta de usuário com privilégios de administrador na instância. Essa é uma proteção no caso de você esquecer a senha de administrador ou ter um problema com a conta de administrador. A nova conta de usuário deve ter permissão para acessar a instância remotamente. Abra System Properties (Propriedades do sistema clicando com o botão direito do mouse no ícone This PC (Este PC) no desktop do Windows ou no Explorador de Arquivos e selecione Properties (Propriedades). Escolha Remote settings (Configurações remotas) e escolha Select Users (Selecionar usuários) para adicionar o usuário ao grupo Remote Desktop Users (Usuários de Desktop Remoto).



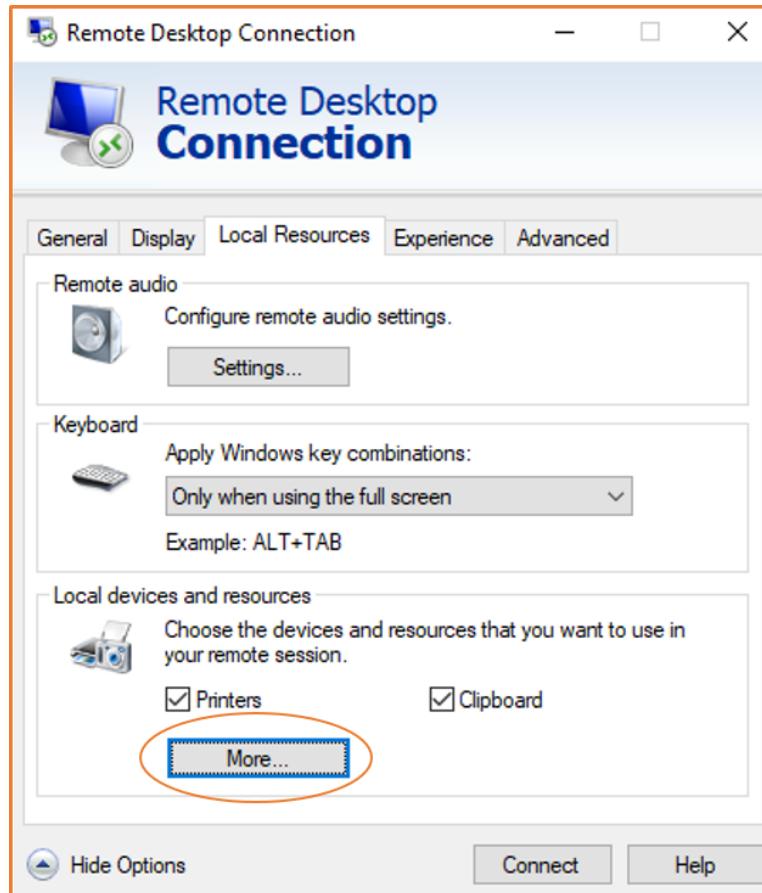
Transferir arquivos para instâncias do Windows

Você pode trabalhar com sua instância Windows da mesma forma que trabalharia com qualquer servidor Windows. Por exemplo, você pode transferir arquivos entre uma instância Windows e seu computador local usando o recurso de compartilhamento de arquivos local do software Microsoft Remote Desktop Connection. Se você habilitar essa opção, poderá acessar seus arquivos locais de suas instâncias Windows. Você pode acessar arquivos locais em unidades de disco rígido, unidades de DVD, unidades de mídia portáteis e unidades de rede mapeadas.

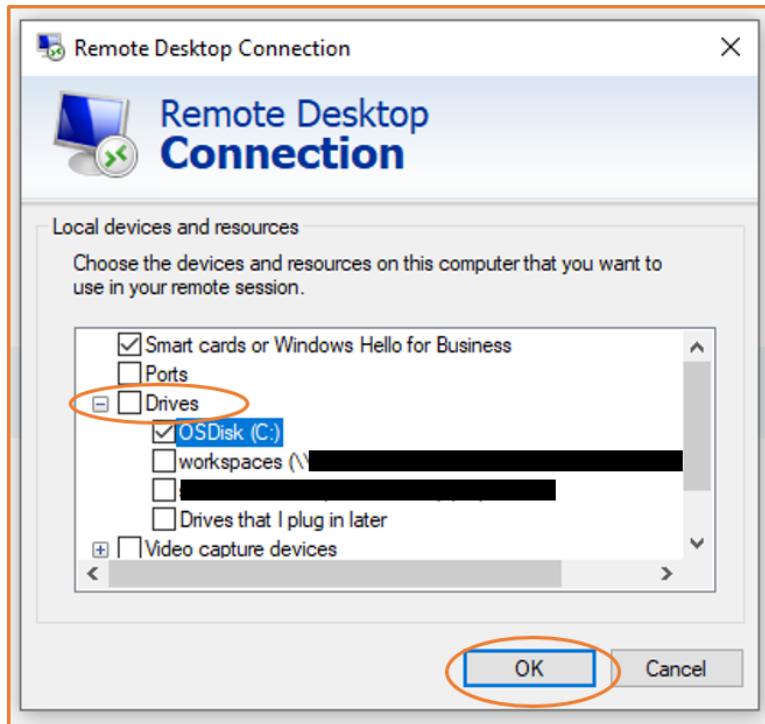
Para disponibilizar recursos e dispositivos locais a uma sessão remota no Windows, mapeie a unidade da sessão remota à unidade local.

Como mapear a unidade de sessão remota à unidade local

1. Abra o cliente de Conexão de Desktop Remoto.
2. Selecione Exibir opções.
3. Selecione a guia Local Resources (Recursos locais).
4. Em Local Devices and resources (Dispositivos e recursos locais), escolha More... (Mais...).



5. Abra Drives (Unidades) e selecione a unidade local à qual mapear sua instância do Windows.
6. Escolha OK.



7. Selecione Connect (Conectar) para se conectar à sua instância do Windows.

Para obter mais informações sobre como disponibilizar dispositivos locais para uma sessão remota em um computador Mac, consulte [Introdução ao Desktop Remoto no Mac](#).

Interromper e iniciar sua instância

Você pode interromper e iniciar a instância se ela tiver um volume do Amazon EBS como seu dispositivo raiz. A instância retém o ID da instância, mas pode ser alterada conforme descrito na seção [Overview \(p. 456\)](#).

Quando você interrompe uma instância, nós a encerramos. Não cobramos pelo uso de uma instância interrompida nem por taxas de transferência de dados, mas cobramos pelo armazenamento dos volumes do Amazon EBS. Toda vez que você inicia uma instância interrompida, cobramos o mínimo de um minuto pelo uso. Após um minuto, cobraremos apenas pelos segundos que você usar. Por exemplo, se você executar uma instância por 20 segundos e, em seguida, interrompê-la, cobraremos por um minuto completo. Se você executar uma instância por 3 minutos e 40 segundos, cobraremos exatamente por esse tempo de uso.

Quando a instância for interrompida, você poderá gerenciar seu volume do dispositivo raiz como qualquer outro volume e também modificá-lo (por exemplo, reparar problemas no sistema de arquivos ou atualizar o software). Basta destacar o volume da instância interrompida, associá-lo a uma instância em execução, fazer suas alterações, destacá-lo da instância em execução e reassocíá-lo à instância interrompida. Reassocie-o usando o nome de dispositivo de armazenamento especificado como dispositivo raiz no mapeamento de dispositivos de blocos para a instância.

Se você decidir que não necessita mais de uma instância, pode encerrá-la. Assim que o estado de uma instância mudar para `shutting-down` ou para `terminated`, interromperemos a cobrança dessa instância. Para obter mais informações, consulte [Encerrar a instância \(p. 474\)](#). Se você preferir hibernar a instância, consulte [Hibernar a instância do Linux sob demanda ou reservada \(p. 459\)](#). Para obter mais informações, consulte [Diferenças entre reinicialização, interrupção, hibernação e encerramento \(p. 416\)](#).

Tópicos

- [Overview \(p. 456\)](#)
- [O que acontece quando você interrompe uma instância \(p. 457\)](#)
- [Interromper e iniciar suas instâncias \(p. 457\)](#)
- [Modificar uma instância interrompida \(p. 458\)](#)
- [Solução de problemas na interrupção da instância \(p. 458\)](#)

Overview

Quando você interrompe uma instância em execução, acontece o seguinte:

- A instância executa um desativação normal e para de ser executada; seu estado muda para `stopping` e depois para `stopped`.
- Todos os volumes do Amazon EBS permanecem associados à instância, e seus dados persistem.
- Todos os dados armazenados na RAM do computador host ou nos volumes do armazenamento de instâncias do computador host se perdem.
- Na maioria dos casos, a instância é migrada para um novo computador host subjacente quando ele é iniciado (embora em alguns casos, permaneça no host atual).
- A instância retém seus endereços IPv4 privados e todos os endereços IPv6 quando interrompida e iniciada. Lançamos o endereço público IPv4 e atribuímos um novo ao iniciá-lo.
- A instância retém os endereços IP elásticos associados. De você são cobrados quaisquer endereços IP elásticos associados a uma instância interrompida. Com o EC2-Classic, um endereço IP elástico é dissociado da sua instância quando você o interrompe. Para obter mais informações, consulte [EC2-Classic \(p. 1099\)](#).
- Quando você interromper e iniciar uma instância do Windows, o serviço EC2Config executará tarefas na instância, como alterar as letras das unidades de qualquer volume do Amazon EBS associado. Para obter mais informações sobre esses padrões e como você pode alterá-los, consulte [Configurar uma instância do Windows usando o serviço EC2Config \(p. 530\)](#).
- Se sua instância estiver em um grupo do Auto Scaling, o serviço do Amazon EC2 Auto Scaling marcará a instância interrompida como não íntegra e poderá encerrá-la e executar uma instância substituta. Para obter mais informações, consulte [Verificações de integridade de instâncias do Auto Scaling](#) no Guia do usuário do Amazon EC2 Auto Scaling.
- Quando você interrompe uma instância ClassicLink, ela se desvincula da VPC à qual estava vinculada. Você deverá vincular novamente a instância à VPC depois de iniciá-la. Para obter mais informações sobre ClassicLink, consulte [ClassicLink \(p. 1107\)](#).

Para obter mais informações, consulte [Diferenças entre reinicialização, interrupção, hibernação e encerramento \(p. 416\)](#).

Você só poderá modificar os atributos a seguir de uma instância quando ela for interrompida:

- Tipo de instância
- Dados do usuário
- Kernel
- Disco RAM

Se você tentar modificar esses atributos enquanto a instância estiver sendo executada, o Amazon EC2 retornará o erro `IncorrectInstanceState`.

O que acontece quando você interrompe uma instância

Quando uma instância do EC2 é interrompida usando o comando `stop-instances`, o seguinte é registrado no nível do SO:

- A solicitação da API envia um evento de pressionamento de botão ao convidado.
- Vários serviços do sistema são interrompidos como resultado do evento de pressionamento de botão. O desligamento normal é acionado pelo evento de pressionamento do botão de desligamento de ACPI do hipervisor.
- O desligamento de ACPI é iniciado.
- A instância será desligada quando o processo de desligamento normal terminar. Não existe um tempo de desligamento configurável para o SO.
- Se o sistema operacional da instância não for encerrado de forma limpa em alguns minutos, um desligamento forçado será executado.

Por padrão, ao iniciar a desativação de uma instância com o Amazon EBS, a instância será interrompida. Você pode alterar esse comportamento para que, em vez disso, seja encerrada. Para obter mais informações, consulte [Alterar o comportamento de desligamento iniciado da instância \(p. 477\)](#).

Interromper e iniciar suas instâncias

Você pode iniciar e interromper a instância baseada em Amazon EBS usando o console ou a linha de comando.

New console

Para parar e iniciar uma instância com Amazon EBS usando o console

1. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.
2. No painel de navegação, escolha Instances e selecione a instância.
3. Escolha Instance state (Estado da instância) e Stop instance (Interromper instância). Se essa opção estiver desabilitada, a instância já foi interrompida ou o dispositivo raiz é um volume de armazenamento de instâncias.
4. Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.
5. (Opcional) Enquanto sua instância estiver interrompida, você poderá modificar determinados atributos de instância. Para obter mais informações, consulte [Modificar uma instância interrompida \(p. 458\)](#).
6. Para iniciar a instância interrompida, selecione a instância e escolha Instance state (Estado da instância) e Start instance (Iniciar instância).
7. Pode demorar alguns minutos para que a instância entre no estado `running`.

Old console

Para parar e iniciar uma instância com Amazon EBS usando o console

1. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.

2. No painel de navegação, escolha Instances e selecione a instância.
3. Escolha Ações, Instance State, Parar. Se essa opção estiver desabilitada, a instância já foi interrompida ou o dispositivo raiz é um volume de armazenamento de instâncias.
4. Quando solicitado a confirmar, escolha Yes, Stop. Pode demorar alguns minutos para que a instância pare.
5. (Opcional) Enquanto sua instância estiver interrompida, você poderá modificar determinados atributos de instância. Para obter mais informações, consulte [Modificar uma instância interrompida \(p. 458\)](#).
6. Para iniciar a instância interrompida, selecione a instância e escolha Actions (Ações), Instance State (Estado da instância), Start (Iniciar).
7. Na caixa de diálogo de confirmação, escolha Sim, iniciar. Pode demorar alguns minutos para que a instância entre no estado running.

Para parar e iniciar uma instância com Amazon EBS usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [stop-instances](#) e [start-instances](#) (AWS CLI)
- [Stop-EC2Instance](#) e [Start-EC2Instance](#) (AWS Tools for Windows PowerShell)

Modificar uma instância interrompida

Você pode alterar o tipo de instância, os dados de usuário e os atributos de otimização do EBS de uma instância interrompida usando o AWS Management Console ou a interface da linha de comando. Você não pode usar o AWS Management Console para modificar os atributos de DeleteOnTermination, kernel ou disco RAM.

Para modificar um atributo da instância

- Para alterar o tipo de instância, consulte [Alterar o tipo de instância \(p. 244\)](#).
- Para alterar os dados do usuário para sua instância, consulte [Trabalhar com dados do usuário da instância \(p. 638\)](#).
- Para habilitar ou desabilitar a otimização do EBS para sua instância, consulte [Modifying EBS–Optimization \(Modificar a otimização do EBS\) \(p. 1457\)](#).
- Para alterar o atributo DeleteOnTermination do volume do dispositivo raiz da sua instância, consulte [Atualizar o mapeamento de dispositivos de blocos de uma instância em execução \(p. 1521\)](#). Não é necessário interromper a instância para alterar esse atributo.

Para modificar um atributo da instância usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

Solução de problemas na interrupção da instância

Se você tiver interrompido sua instância com Amazon EBS e ela aparentar estar "presa" no estado stopping, você poderá pará-la à força. Para obter mais informações, consulte [Solução de problemas na interrupção da instância \(p. 1602\)](#).

Hibernar a instância do Linux sob demanda ou reservada

Ao hibernar uma instância, o Amazon EC2 indica a realização da hibernação (suspend-to-disk) ao sistema operacional. A hibernação salva os conteúdos da memória da instância (RAM) para o volume raiz do Amazon Elastic Block Store (Amazon EBS). O Amazon EC2 persiste o volume raiz do EBS e todos os volumes de dados do EBS anexados. Quando você inicia sua instância:

- O volume raiz do EBS é restaurado para seu estado anterior
- Os conteúdos da RAM são recarregados
- Os processos que estavam em execução anteriormente na instância são retomados
- Os volumes de dados anexados anteriormente são reanexados e a instância conserva seu ID de instância.

É possível hibernar uma instância apenas se ela estiver [habilitada para hibernação \(p. 463\)](#) e atender aos [pré-requisitos de hibernação \(p. 460\)](#).

Se uma instância ou aplicação levar muito tempo para o bootstrap e criar um espaço de memória para se tornar totalmente produtivo, você poderá usar a hibernação para preaquecer a instância. Para pré-aquecer a instância:

1. Execute-a com a hibernação habilitada.
2. Coloque-a em um estado desejado.
3. Deixe-a em hibernação para que ela fique pronta para ser retomada no estado desejado sempre que necessário.

Você não é cobrado pelo uso de uma instância hibernada quando ela está no estado `stopped`. Porém, você será cobrado pelo uso da instância enquanto ela estiver no estado `stopping`, enquanto o conteúdo da RAM é transferido para o volume raiz do EBS. (Isso é diferente de quando você [interrompe uma instância \(p. 455\)](#) sem hiberná-la.) Você não é cobrado pela transferência de dados. No entanto, cobramos pelo armazenamento de volumes do EBS, incluindo o armazenamento de conteúdos da RAM.

Se não precisar mais de uma instância, você pode encerrá-la a qualquer momento, incluindo quando ela está em um estado `stopped` (em hibernação). Para obter mais informações, consulte [Encerrar a instância \(p. 474\)](#).

Note

Para obter informações sobre como usar a hibernação em instâncias do Linux, consulte [Hibernar a instância do Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

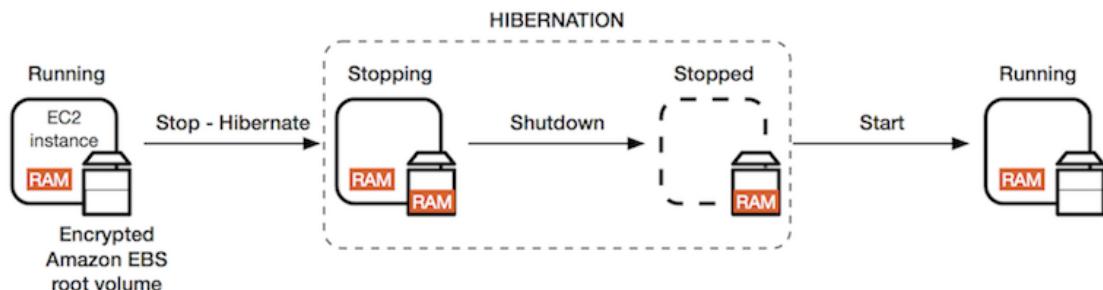
Para obter informações sobre o Instâncias spot em hibernação, consulte [Hibernar Instâncias spot interrompida \(p. 338\)](#).

Tópicos

- [Visão geral da hibernação \(p. 460\)](#)
- [Pré-requisitos de hibernação \(p. 460\)](#)
- [Limitations \(p. 463\)](#)
- [Habilitar a hibernação para uma instância \(p. 463\)](#)
- [Hibernar uma instância \(p. 466\)](#)
- [Iniciar um instância em hibernação \(p. 468\)](#)
- [Solucionar problemas de hibernação \(p. 469\)](#)

Visão geral da hibernação

O diagrama a seguir mostra uma visão geral básica do processo de hibernação.



Quando você hiberna uma instância em execução, acontece o seguinte:

- Quando você inicia a hibernação, a instância muda para o estado **stopping**. O Amazon EC2 sinaliza o sistema operacional para realizar a hibernação (suspend-to-disk). A hibernação congela todos os processos, salva o conteúdo da RAM no volume raiz do EBS e, depois, executa um desligamento normal.
- Quando o desligamento é concluído, a instância muda para o estado **stopped**.
- Todos os volumes do EBS permanecem anexados à instância, e seus dados são mantidos, incluindo o conteúdo salvo da RAM.
- Todos os volumes de armazenamento de instâncias do Amazon EC2 permanecem associados à instância, mas os dados nos volumes de armazenamento de instância são perdidos.
- Na maioria dos casos, a instância é migrada para um novo computador host subjacente quando ele é iniciado. Isso também acontece ao interromper e iniciar uma instância.
- Quando a instância é iniciada, ela é inicializada, e o sistema operacional lê o conteúdo da RAM no volume raiz do EBS antes de descongelar os processos para retomar seu estado.
- A instância retém seus endereços IPv4 privados e todos os endereços IPv6. Quando você inicia a instância, ela continua a manter seus endereços IPv4 privados e todos os endereços IPv6.
- O Amazon EC2 libera o endereço IPv4 público. Quando você inicia a instância, o Amazon EC2 atribui um novo endereço IPv4 público à instância.
- A instância retém os endereços IP elásticos associados. Você é cobrado por todos os endereços IP elásticos associados a uma instância em hibernação. Com o EC2-Classic, um endereço IP elástico é dissociado da instância quando você a coloca para hibernar. Para obter mais informações, consulte [EC2-Classic \(p. 1099\)](#).
- Quando você hiberna uma instância ClassicLink, ela se desvincula da VPC à qual estava vinculada. Você deverá vincular novamente a instância à VPC depois de iniciá-la. Para obter mais informações, consulte [ClassicLink \(p. 1107\)](#).

Para obter informações sobre como a hibernação difere da reinicialização, da interrupção e do encerramento, consulte [Diferenças entre reinicialização, interrupção, hibernação e encerramento \(p. 416\)](#).

Pré-requisitos de hibernação

Para hibernar uma instância sob demanda ou Instância reservada, os seguintes pré-requisitos devem estar implementados:

- [AMIs compatíveis Windows \(p. 461\)](#)
- [Famílias de instâncias compatíveis \(p. 461\)](#)

- [Tamanho da instância \(p. 462\)](#)
- [Tamanho da instância RAM \(p. 462\)](#)
- [Tipo do volume de raiz \(p. 462\)](#)
- [Tamanho do volume raiz do EBS \(p. 462\)](#)
- [Tipos de volume EBS compatíveis \(p. 462\)](#)
- [Criptografia do volume raiz EBS \(p. 462\)](#)
- [Ativar hibernação no lançamento \(p. 462\)](#)
- [Opções de compra \(p. 463\)](#)

AMIs compatíveis Windows

Deve ser uma AMI do HVM que ofereça suporte à hibernação:

- AMI do Windows Server 2012 lançada em 11/09/2019 ou posterior.
- AMI do Windows Server 2012 R2 lançada em 11/09/2019 ou posterior.
- AMI do Windows Server 2016 lançada em 11/09/2019 ou posterior.
- AMI do Windows Server 2019 lançada em 11/09/2019 ou posterior.

Para obter informações sobre as AMIs Linux compatíveis, consulte [AMIs compatíveis com o Linux](#) no Manual do usuário do Amazon EC2 para instâncias do Linux.

Famílias de instâncias compatíveis

- Xen: C3, C4, I3, M3, M4, R3, R4, T2
- Nitro: C5, C5d, M5, M5a, M5ad, M5d, R5, R5a, R5ad, R5d, T3*, T3a*

* Para hibernação, recomendamos que você use uma instância T3 ou T3a com pelo menos 1 GB de RAM.

Para ver os tipos de instância disponíveis que suportam hibernação em uma Região específica

Os tipos de instância disponíveis variam de acordo com a região. Para ver os tipos de instâncias disponíveis que suportam hibernação em uma Região, use o comando `describe-instance-types` com o parâmetro `--region`. Inclua o parâmetro `--filters` para ver apenas os tipos de instância que suportam hibernação.

```
C:\> aws ec2 describe-instance-types \
--region us-east-2 \
--filters Name=hibernation-supported,Values=true \
--query "InstanceTypes[*].[InstanceType]" \
--output table
```

Exemplo de saída

```
-----+
|DescribeInstanceTypes|
+-----+
| r5a.xlarge      |
| c4.4xlarge     |
| m5ad.large     |
| c5.4xlarge      |
| m4.4xlarge      |
| t3.2xlarge      |
```

...

Tamanho da instância

Não há suporte para instâncias bare metal.

Tamanho da instância RAM

Pode ter até 16 GB.

Tipo do volume de raiz

Deve ser um volume do EBS, e não um volume de armazenamento de instâncias.

Tamanho do volume raiz do EBS

Deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar o uso esperado; sistema operacional ou aplicações, por exemplo. Quando você habilita a hibernação, é alocado espaço no volume raiz na inicialização para armazenar a RAM.

Tipos de volume EBS compatíveis

- SSD para uso geral (gp2 e gp3)
- IOPS provisionado SSD (io1 e io2)

Se você escolher um tipo de volume SSD de IOPS Provisionado SSD, você deverá provisionar o volume do EBS com as IOPS apropriadas para alcançar a performance ideal para hibernação. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#).

Criptografia do volume raiz EBS

Para usar a hibernação, o volume raiz deve ser criptografado para garantir a proteção do conteúdo confidencial que estiver na memória no momento da hibernação. Quando os dados da RAM são movidos para o volume raiz do EBS, eles sempre são criptografados. A criptografia do volume raiz é imposta na execução da instância.

Use uma das três opções a seguir para garantir que o volume raiz seja um volume criptografado do EBS:

- Criptografia do EBS por padrão: você pode habilitar a criptografia do EBS por padrão para garantir que todos os novos volumes do EBS criados na sua conta da AWS sejam criptografados. Dessa forma, você habilita a hibernação para suas instâncias sem especificar a intenção da criptografia na execução da instância. Para obter mais informações, consulte [Criptografia por padrão \(p. 1426\)](#).
- Criptografia EBS de uma “única etapa”: você pode iniciar instâncias do EC2 criptografadas com suporte de EBS a partir de uma AMI não criptografada e, ao mesmo tempo, habilitar a hibernação. Para obter mais informações, consulte [Usar criptografia com AMIs com EBS \(p. 135\)](#).
- AMI criptografada: você pode habilitar a criptografia do EBS usando uma AMI criptografada para iniciar sua instância. Se a sua AMI não tiver um snapshot raiz criptografado, você poderá copiá-lo para uma nova AMI e solicitar a criptografia. Para obter mais informações, consulte [Criptografar uma imagem não criptografada durante a cópia \(p. 139\)](#) e [Copiar um AMI \(p. 122\)](#).

Ativar hibernação no lançamento

Não é possível habilitar a hibernação em uma instância pré-existente (em execução ou parada). Para obter mais informações, consulte [Habilitar a hibernação para uma instância \(p. 463\)](#).

Opções de compra

Esse recurso está disponível apenas para Instâncias sob demanda e instâncias reservadas. Ele não está disponível no Instâncias spot. Para obter informações sobre as Instâncias spot em hibernação, consulte [Hibernar Instâncias spot interrompida \(p. 338\)](#).

Limitations

- Quando você hiberna uma instância, os dados em todos os volumes de armazenamento de instâncias são perdidos.
- Não é possível hibernar uma instância com mais de 16 GB de RAM.
- Se você criar um snapshot ou uma AMI a partir de uma instância que está hibernada ou que tenha hibernação ativada, talvez não consiga se conectar à instância.
- Você não pode alterar o tipo de instância ou o tamanho de uma instância quando a hibernação está ativada.
- Não é possível hibernar uma instância que está em um grupo do Auto Scaling ou é usada pelo Amazon ECS. Se sua instância estiver em um grupo do Auto Scaling, e você tentar hiberná-la, o serviço Amazon EC2 Auto Scaling marcará a instância interrompida como não íntegra e poderá encerrá-la e executar uma instância substituta. Para obter mais informações, consulte [Verificações de integridade de instâncias do Auto Scaling](#) no Guia do usuário do Amazon EC2 Auto Scaling.
- Não é possível hibernar uma instância configurada para inicializar no modo UEFI.
- Se você hibernar uma instância que foi executada em um Reserva de capacidade, o Reserva de capacidade não garante que a instância hibernada possa retornar depois de tentar iniciá-la.
- Não oferecemos suporte à manutenção de uma instância em hibernação por mais de 60 dias. Para manter a instância por mais que 60 dias, inicie, interrompa e inicialize a instância em hibernação.
- Atualizamos constantemente nossa plataforma com atualizações e patches de segurança, o que entra em conflito com instâncias em hibernação. Notificamos você sobre as atualizações críticas que exigam uma inicialização das instâncias em hibernação para que você possa executar um desligamento ou uma reinicialização para aplicar as atualizações e os patches de segurança necessários.

Habilitar a hibernação para uma instância

Para colocar uma instância em hibernação, é necessário habilitá-la para hibernação ao iniciar a instância.

Important

Não é possível habilitar ou desabilitar a hibernação para uma instância depois de executá-la.

Console

Para habilitar a hibernação usando o console

1. Siga o procedimento do [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).
2. Na página Choose an Amazon Machine Image (AMI) (Escolher uma Imagem de máquina da Amazon (AMI)), selecione uma AMI compatível com a hibernação. Para obter mais informações sobre as AMIs compatíveis, consulte [Pré-requisitos de hibernação \(p. 460\)](#).
3. Na página Choose an Instance Type (Escolher um tipo de instância), selecione um tipo de instância compatível e escolha Next: Configure Instance Details (Próximo: configurar os detalhes da instância). Para obter mais informações sobre os tipos de instância compatíveis, consulte [Pré-requisitos de hibernação \(p. 460\)](#).
4. Na página Configure Instance Details (Configurar detalhes da instância), em Stop - Hibernate Behavior (Interromper - comportamento de hibernação), marque a caixa de seleção Enable

hibernation as an additional stop behavior (Habilitar a hibernação como um comportamento de interrupção adicional).

5. Na página Adicionar armazenamento, para o volume raiz, especifique as seguintes informações:
 - Para Size (GiB) (Tamanho (GiB)), insira o tamanho do volume raiz do EBS. O volume deve ser grande o suficiente para armazenar o conteúdo da RAM e acomodar o uso esperado.
 - Para Volume Type (Tipo de volume), selecione um tipo de volume do EBS compatível (SSD de uso geral (gp2 e gp3) ou SSD de IOPS provisionadas (io1 e io2)).
 - Para Criptografia, selecione a chave de criptografia para o volume. Se tiver habilitado a criptografia por padrão nessa região da AWS, a criptografia padrão será selecionada.

Para obter mais informações sobre os pré-requisitos para o volume raiz, consulte [Pré-requisitos de hibernação \(p. 460\)](#).

6. Continue como solicitado pelo assistente. Ao terminar de revisar suas opções na página Review Instance Launch (Revisar execução da instância), selecione Launch (Executar). Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).

AWS CLI

Para habilitar a hibernação usando a AWS CLI

Use o comando [run-instances](#) para executar uma instância. Especifique os parâmetros do volume raiz do EBS usando o parâmetro `--block-device-mappings file://mapping.json` e habilite a hibernação usando o parâmetro `--hibernation-options Configured=true`.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

Especifique o seguinte em `mapping.json`.

```
[{"DeviceName": "/dev/xvda",
  "Ebs": {
    "VolumeSize": 30,
    "VolumeType": "gp2",
    "Encrypted": true
  }
}]
```

Note

O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando [describe-images](#).

```
aws ec2 describe-images --image-id ami-0abcdef1234567890
```

Se você habilitou a criptografia por padrão nesta região da AWS, você pode omitir `"Encrypted": true`.

PowerShell

Para habilitar a hibernação usando a AWS Tools for Windows PowerShell

Use o comando [New-EC2Instance](#) para executar uma instância. Especifique o volume raiz do EBS definindo primeiro o mapeamento do dispositivo de bloco e adicionando-o ao comando usando o parâmetro `-BlockDeviceMappings`. Habilite a hibernação usando o parâmetro `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance ` 
    -ImageId ami-0abcdef1234567890 ` 
    -InstanceType m5.large ` 
    -BlockDeviceMappings $ebs_encrypt ` 
    -HibernationOptions_Configured $true ` 
    -MinCount 1 ` 
    -MaxCount 1 ` 
    -KeyName MyKeyPair
```

Note

O valor para `DeviceName` deve corresponder ao nome do dispositivo raiz associado à AMI. Para localizar o nome do dispositivo raiz, use o comando [Get-EC2Image](#).

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Se você habilitou a criptografia por padrão nesta região da AWS, poderá omitir o `Encrypted = $true` do mapeamento do dispositivo de bloco.

New console

Para visualizar se uma instância está habilitada para hibernação no console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, na guia Details (Detalhes), na seção Instance details (Detalhes da instância), verifique Stop-hibernate behavior (Interromper - comportamento de hibernação). Enabled (Habilitada) indica que a instância está habilitada para hibernação.

Old console

Para visualizar se uma instância está habilitada para hibernação no console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, no painel de detalhes, inspecione Stop - Hibernation behavior (Interromper - comportamento de hibernação). Enabled (Habilitada) indica que a instância está habilitada para hibernação.

AWS CLI

Para visualizar se uma instância está habilitada para hibernação usando a AWS CLI

Use o comando [describe-instances](#) e especifique o parâmetro `--filters "Name=hibernation-options.configured,Values=true"` para filtrar as instâncias que estão habilitadas para hibernação.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

O campo da saída a seguir indica que a instância está habilitada para hibernação.

```
"HibernationOptions": {
    "Configured": true
}
```

PowerShell

Para visualizar se uma instância está habilitada para hibernação usando a AWS Tools for Windows PowerShell

Use o comando [Get-EC2Instance](#) e especifique o parâmetro `-Filter @{ Name="hibernation-options.configured"; Value="true"}` para filtrar as instâncias que estão habilitadas para hibernação.

```
Get-EC2Instance ^
    -Filter @{ Name="hibernation-options.configured"; Value="true"}
```

A saída lista as instâncias do EC2 habilitadas para hibernação.

Hibernar uma instância

É possível hibernar uma instância se ela estiver [habilitada para hibernação \(p. 463\)](#) e atender aos [pré-requisitos de hibernação \(p. 460\)](#). Se uma instância não puder hibernar com sucesso, ocorrerá um desligamento normal.

New console

Para hibernar uma instância com suporte do Amazon EBS usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e escolha Instance state (Estado da instância) e Hibernate instance (Hibernar instância). Se Hibernate instance (Hibernar instância) estiver desabilitado, a instância já estará em hibernação ou interrompida ou não poderá ser hibernada. Para obter mais informações, consulte [Pré-requisitos de hibernação \(p. 460\)](#).
4. Quando a confirmação for solicitada, escolha Hibernate (Hibernar). Pode demorar alguns minutos para que a instância hiberne. O estado da instância primeiro muda para Interrompendo e, em seguida, muda para Interrompido quando a instância tiver hibernado.

Old console

Para hibernar uma instância com suporte do Amazon EBS usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e escolha Actions (Ações), Instance State (Estado da instância) e Stop - Hibernate (Interromper - hibernar). Se Stop - Hibernate (Interromper - hibernar) estiver desabilitado, a instância já estará em hibernação ou interrompida ou não poderá ser hibernada. Para obter mais informações, consulte [Pré-requisitos de hibernação \(p. 460\)](#).
4. Na caixa de diálogo de confirmação, escolha Yes, Stop - Hibernate (Sim, parar - hibernar). Pode demorar alguns minutos para que a instância hiberne. O Estado da instância primeiro muda para Interrompendo e, em seguida, muda para Interrompido quando a instância tiver hibernado.

AWS CLI

Para hibernar uma instância com suporte do Amazon EBS usando a AWS CLI

Use o comando [stop-instances](#) e especifique o parâmetro --hibernate.

```
aws ec2 stop-instances \
--instance-ids i-1234567890abcdef0 \
--hibernate
```

PowerShell

Para hibernar uma instância com suporte do Amazon EBS usando a AWS Tools for Windows PowerShell

Use o comando [Stop-EC2Instance](#) e especifique o parâmetro -Hibernate \$true.

```
Stop-EC2Instance ^
-InstanceId i-1234567890abcdef0 ^
-Hibernate $true
```

New console

Para visualizar se a hibernação foi iniciada em uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, na guia Details (Detalhes), na seção Instance details (Detalhes da instância), verifique State transition message (Mensagem de transição de estado). A mensagem Client.UserInitiatedHibernate: User initiated hibernate (Client.UserInitiatedHibernate: hibernação iniciada pelo usuário) indica que a hibernação foi iniciada na instância.

Old console

Para visualizar se a hibernação foi iniciada em uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, no painel de detalhes, inspecione State transition reason message (Mensagem de motivo de transição de estado). A mensagem Client.UserInitiatedHibernate: User initiated hibernate (Client.UserInitiatedHibernate: hibernação iniciada pelo usuário) indica que a hibernação foi iniciada na instância.

AWS CLI

Para visualizar se a hibernação foi iniciada em uma instância usando a AWS CLI

Use o comando **describe-instances** e especifique o filtro **state-reason-code** para ver as instâncias nas quais a hibernação foi iniciada.

```
aws ec2 describe-instances \
--filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

O seguinte campo da saída indica que a hibernação foi iniciada na instância.

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

Para visualizar se a hibernação foi iniciada em uma instância usando a AWS Tools for Windows PowerShell

Use o comando **Get-EC2Instance** e especifique o filtro **state-reason-code** para ver as instâncias nas quais a hibernação foi iniciada.

```
Get-EC2Instance ^
-Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

A saída lista as instâncias do EC2 nas quais a hibernação foi iniciada.

Iniciar um instância em hibernação

Inicie uma instância em hibernação da mesma maneira como faria em uma instância interrompida.

New console

Como iniciar uma instância em hibernação usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância em hibernação e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Pode demorar alguns minutos para que a instância entre no estado **running**. Durante esse tempo, as [verificações de status \(p. 868\)](#) da instância mostram a instância em um estado de falha até que a instância seja iniciada.

Old console

Como iniciar uma instância em hibernação usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância em hibernação e escolha Actions (Ações), Instance State (Estado da instância) e Start (Iniciar). Pode demorar alguns minutos para que a instância entre no estado

running. Durante esse tempo, as [verificações de status \(p. 868\)](#) da instância mostram a instância em um estado de falha até que a instância seja iniciada.

AWS CLI

Como iniciar uma instância em hibernação usando o AWS CLI

Use o comando [start-instances](#).

```
aws ec2 start-instances \
--instance-ids i-1234567890abcdef0
```

PowerShell

Como iniciar uma instância em hibernação usando o AWS Tools for Windows PowerShell

Use o comando [Start-EC2Instance](#).

```
Start-EC2Instance ^
-InstanceId i-1234567890abcdef0
```

Solucionar problemas de hibernação

Use estas informações para ajudar a diagnosticar e corrigir problemas que podem ser encontrados ao hibernar uma instância.

Não é possível hibernar imediatamente após a execução

Você receberá uma mensagem de erro se tentar hibernar uma instância muito rapidamente depois de executá-la.

Aguarde por cerca de cinco minutos depois da execução para hiberná-la.

A transição de stopping para stopped demora muito tempo, e o estado da memória não é restaurado depois da execução

Quando demora muito tempo para que a instância em hibernação faça a transição do estado `stopping` para `stopped`, e se o estado da memória não é restaurado depois da execução, isso pode indicar que a hibernação não foi configurada corretamente.

Windows Server 2016 e posterior

Verifique o log de execução do EC2 e procure mensagens relacionadas à hibernação. Para acessar o log de execução do EC2, [conecte-se \(p. 443\)](#) à instância e abra o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log` em um editor de texto.

Note

Por padrão, o Windows oculta os arquivos e as pastas sob `C:\ProgramData`. Para visualizar os diretórios e os arquivos do EC2, insira o caminho no Windows Explorer ou altere as propriedades da pasta para exibir os arquivos e as pastas ocultos.

Localize as linhas do log para hibernação. Se as linhas do log indicarem uma falha ou se não houver linhas no log, muito provavelmente terá ocorrido uma falha na configuração da hibernação na execução.

Por exemplo, a seguinte mensagem indica que ocorreu uma falha ao configurar a hibernação: **Message: Failed to enable hibernation.**

Se a linha do log contiver **HibernationEnabled: true**, a hibernação terá sido configurada com êxito.

Windows Server 2012 R2 e anteriores

Verifique o log de configuração do EC2 e procure mensagens relacionadas à hibernação. Para acessar o log de configuração do EC2, [conecte-se \(p. 443\)](#) à instância e abra o arquivo C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt em um editor de texto. Localize as linhas do log para **SetHibernateOnSleep**. Se as linhas do log indicarem uma falha ou se não houver linhas no log, muito provavelmente terá ocorrido uma falha na configuração da hibernação na execução.

Por exemplo, a seguinte mensagem indica que o volume raiz da instância não é grande o suficiente: **SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.**

Se a linha do log for **SetHibernateOnSleep: HibernationEnabled: true**, a hibernação terá sido configurada com êxito.

Se você não vir nenhum log desses processos, talvez sua AMI não ofereça suporte à hibernação. Para obter informações sobre as AMIs compatíveis, consulte [Pré-requisitos de hibernação \(p. 460\)](#).

Tamanho da instância

Se você estiver usando uma instância T3 ou T3a com menos de 1 GB de RAM, tente aumentar o tamanho da instância para uma que tenha pelo menos 1 GB de RAM.

Instância "presa" no estado de parada

Se você tiver hibernado sua instância e ela aparentar estar "presa" no estado **stopping**, você poderá interrompê-la à força. Para obter mais informações, consulte [Solução de problemas na interrupção da instância \(p. 1602\)](#).

Reiniciar a instância

Reiniciar a instância equivale a reiniciar o sistema operacional. Na maioria dos casos, leva apenas alguns minutos para reiniciar sua instância. Quando você reinicia uma instância, ela mantém seu nome DNS público (IPv4), o endereço IPv4 privado e público, o endereço IPv6 (se aplicável) e quaisquer dados nos volumes de armazenamento de instâncias.

A reinicialização de uma instância não inicia um novo período (com uma cobrança mínima de um minuto) de faturamento de instância, diferentemente do que acontece na interrupção e na inicialização da instância.

Nós pudemos programar sua instância para uma reinicialização para manutenção necessária, como para aplicar atualizações que exigem uma reinicialização. Nenhuma ação é necessária da sua parte; recomendamos que você espere a reinicialização ocorrer dentro da janela programada. Para obter mais informações, consulte [Eventos programados para instâncias \(p. 874\)](#).

Recomendamos que você use o console do Amazon EC2 uma ferramenta de linha de comando ou a API do Amazon EC2 para reiniciar sua instância, em vez de executar o comando de reinicialização do sistema operacional pela sua instância. Se você usar o console do Amazon EC2, uma ferramenta de linha de comando ou a API do Amazon EC2 para reiniciar sua instância, executaremos uma reinicialização

forçada se a instância não fechar corretamente em alguns minutos. Se você usar o AWS CloudTrail e, em seguida, usar o Amazon EC2 para reinicializar sua instância também criará um registro de API de quando a instância foi reinicializada.

Se o Windows está instalando atualizações em sua instância, recomendamos que você não reinicie ou feche sua instância usando o console Amazon EC2 ou a linha de comando até que todas as atualizações estejam instaladas. Ao usar o console ou a linha de comando Amazon EC2 para reinicializar ou fechar sua instância, há risco que sua instância seja reinicializada forçadamente. Uma "hard reboot" enquanto as atualizações estão sendo instaladas poderia colocar suas instâncias em um estado instável.

New console

Para reinicializar uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Instance State (Estado da instância), Reboot instance (Reiniciar a instância).
4. Escolha Reboot (Reiniciar) quando a confirmação for solicitada. A instância permanece no estado em execução.

Old console

Para reinicializar uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Instance State (Estado da instância) e Reboot (Reiniciar).
4. Escolha Yes, Reboot (Sim, reiniciar) quando a confirmação for solicitada. A instância permanece no estado em execução.

Para reinicializar uma instância usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [reboot-instances](#) (AWS CLI)
- [Restart-EC2Instance](#) (AWS Tools for Windows PowerShell)

Desativação da instância

A instância é programada para ser desativada quando a AWS detecta uma falha irreparável do hardware subjacente que hospeda a instância. Quando uma instância atinge sua data de desativação programada, ela é pela AWS. Se o dispositivo raiz da instância estiver em um volume do Amazon EBS, a instância será interrompida e você poderá reiniciá-la a qualquer momento. Iniciar a instância interrompida migra-a para o novo hardware.

Para obter mais informações sobre os tipos de eventos de instância, consulte [Eventos programados para instâncias \(p. 874\)](#).

Tópicos

- [Identificar instâncias programadas para desativação \(p. 472\)](#)

- [Ações a serem executadas para instâncias programadas para desativação \(p. 473\)](#)

Identificar instâncias programadas para desativação

Se a sua instância estiver programada para desativação, você receberá um e-mail antes do evento com o ID e a data de desativação da instância. Você também pode verificar se há instâncias programadas para desativação usando o console do Amazon EC2 ou a linha de comando.

Important

Se uma instância estiver programada para desativação, recomendamos que você aja o mais rápido possível, pois a instância poderá ficar inacessível. (A notificação por e-mail que você recebe indica o seguinte: "Devido a essa degradação, sua instância já pode estar inacessível.") Para obter mais informações sobre a ação recomendada que você deve executar, consulte [Check if your instance is reachable](#).

Formas de identificar instâncias programadas para desativação

- [Notificação por e-mail \(p. 472\)](#)
- [Identificação do console \(p. 472\)](#)

Notificação por e-mail

Se a sua instância estiver programada para desativação, você receberá um e-mail antes do evento com o ID e a data de desativação da instância.

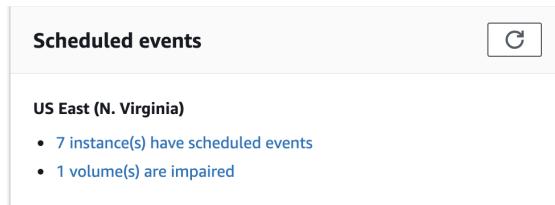
O e-mail é enviado ao titular da conta principal e ao contato de operações. Para obter mais informações, consulte [Adding, changing, or removing alternate contacts \(Adicionar, alterar ou remover contatos alternativos\)](#) no AWS Billing and Cost Management User Guide (Manual do usuário do AWS Billing and Cost Management).

Identificação do console

Se você usa uma conta de e-mail que não verifica regularmente, por exemplo, notificações de desativação, use o console do Amazon EC2 ou a linha de comando para determinar se alguma de suas instâncias estão programadas para desativação.

Para identificar as instâncias agendadas para desativação usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2). Em Scheduled events (Eventos agendados), é possível ver os eventos associados a volumes e instâncias do Amazon EC2, organizados por região.



3. Se você tiver uma instância com um evento agendado listado, selecione o link abaixo do nome da região para acessar a página Events (Eventos).
4. A página Events (Eventos) lista todos os recursos com eventos associados a eles. Para visualizar as instâncias que estão agendadas para desativação, selecione Instance resources (Recursos

da instância) na primeira lista de filtros e, em seguida, Instance stop or retirement (Interrupção ou desativação de instância) na segunda lista de filtros.

5. Se os resultados do filtro mostrarem que uma instância está agendada para desativação, selecione-a e anote a data e a hora do campo Start time (Hora de início) no painel de detalhes. Essa é a data de desativação da instância.

Para identificar as instâncias agendadas para desativação usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [describe-instance-status](#) (AWS CLI)
- [Get-EC2InstanceState](#) (AWS Tools for Windows PowerShell)

Ações a serem executadas para instâncias programadas para desativação

Para preservar os dados em sua instância sendo desativada, é possível executar uma das ações a seguir. É importante que você execute essa ação antes da data de desativação da instância, para evitar períodos de desativação e perda de dados imprevistos.

Verifique se sua instância está acessível

Quando você for notificado de que sua instância está programada para desativação, recomendamos que execute a seguinte ação o mais rápido possível:

- Verifique se sua instância está acessível [conectando-se \(p. 443\)](#) ou fazendo ping na instância.
- Se sua instância estiver acessível, planeje interromper/iniciar a instância em um momento apropriado antes da data de desativação programada, quando o impacto for mínimo. Para obter mais informações sobre como interromper e iniciar sua instância e o que esperar quando a instância é interrompida, como o efeito em endereços IP elásticos, públicos e privados associados à instância, consulte [Interromper e iniciar sua instância \(p. 455\)](#). Observe que os dados em volumes de armazenamento de instâncias são perdidos quando você interrompe e inicia sua instância.
- Se sua instância estiver inacessível, você deverá agir imediatamente e executar uma [interrupção/inicialização \(p. 455\)](#) para recuperar sua instância.
- Se preferir [encerrar \(p. 474\)](#) sua instância, planeje fazê-lo o mais rápido possível, para que você pare de receber cobranças pela instância.

Crie um backup da sua instância

Crie uma AMI baseada em EBS em sua instância para que você tenha um backup. Para garantir a integridade dos dados, interrompa a instância antes de criar a AMI. Espere a data de desativação agendada para a interrupção da instância ou interrompa a instância por conta própria antes dessa data. Você pode iniciar a instância novamente a qualquer momento. Para obter mais informações, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#).

Execute uma instância de substituição

Depois de criar uma AMI a partir da sua instância, você pode usar a AMI para iniciar uma instância de substituição. No console do Amazon EC2, selecione sua nova AMI e escolha Actions (Ações), Launch (Iniciar). Siga o assistente para executar sua instância. Para obter mais informações sobre cada etapa do assistente, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).

Encerrar a instância

Você pode excluir sua instância quando não precisar mais dela. Isso é chamado de encerrar sua instância. Assim que o estado de uma instância mudar para `shutting-down` ou para `terminated`, não haverá mais custos para essa instância.

Não é possível conectar-se a uma instância ou iniciá-la depois de interrompê-la. No entanto, você pode executar instâncias adicionais usando a mesma AMI. Se você preferir interromper e iniciar a instância ou hiberná-la, consulte [Interromper e iniciar sua instância \(p. 455\)](#) ou [Hibernar a instância do Linux sob demanda ou reservada \(p. 459\)](#). Para obter mais informações, consulte [Diferenças entre reinicialização, interrupção, hibernação e encerramento \(p. 416\)](#).

Tópicos

- [Encerramento de instância \(p. 474\)](#)
- [Terminar várias instâncias com proteção contra término entre zonas de disponibilidade \(p. 475\)](#)
- [O que acontece quando você encerra uma instância \(p. 475\)](#)
- [Como encerrar uma instância \(p. 475\)](#)
- [Habilitar a proteção contra encerramento \(p. 476\)](#)
- [Alterar o comportamento de desligamento iniciado da instância \(p. 477\)](#)
- [Preservar volumes do Amazon EBS no encerramento da instância \(p. 478\)](#)

Encerramento de instância

Depois de encerrar uma instância, ela permanecerá visível no console por um curto período, quando será automaticamente excluída. Você não pode excluir a entrada da instância encerrada por conta própria. Depois que uma instância é interrompida, recursos como tags e volumes são gradualmente dissociados da instância e podem não ficar visíveis na instância interrompida após um breve período.

Quando uma instância é encerrada, os dados em quaisquer volumes de armazenamento de instâncias associados a ela são excluídos.

Por padrão, os volumes do dispositivo raiz do Amazon EBS são excluídos automaticamente quando a instância é encerrada. Contudo, por padrão, todos os volumes do EBS adicionais que você anexar na execução ou todos os volumes do EBS que você anexar a uma instância existente persistirão mesmo após o encerramento da instância. Esse comportamento é controlado pelo atributo `DeleteOnTermination` do volume, que você pode modificar. Para obter mais informações, consulte [Preservar volumes do Amazon EBS no encerramento da instância \(p. 478\)](#).

Você pode impedir que uma instância seja encerrada acidentalmente por alguém usando o AWS Management Console, a CLI e a API. Esse recurso está disponível para instâncias com Amazon EBS e instâncias com armazenamento de instâncias do Amazon EC2. Cada instância tem um atributo `DisableApiTermination` com o valor padrão de `false` (ela pode ser encerrada pelo Amazon EC2). Você pode modificar esse atributo enquanto a instância estiver sendo executada ou interrompida (no caso de instâncias baseadas no Amazon EBS). Para obter mais informações, consulte [Habilitar a proteção contra encerramento \(p. 476\)](#).

Você pode definir se uma instância deve ser interrompida ou encerrada quando o desligamento for iniciado a partir da instância usando um comando do sistema operacional para o desligamento do sistema. Para obter mais informações, consulte [Alterar o comportamento de desligamento iniciado da instância \(p. 477\)](#).

Se você executar um script no encerramento da instância, ela pode ter uma interrupção anormal, pois não há como garantir que os scripts de desativação sejam executados. O Amazon EC2 tenta desativar uma instância corretamente e executar quaisquer scripts de desativação do sistema. No entanto, determinados

eventos (como falha de hardware) podem impedir que esses scripts de desativação do sistema sejam executados.

Terminar várias instâncias com proteção contra término entre zonas de disponibilidade

Se você terminar várias instâncias em várias zonas de disponibilidade e uma ou mais instâncias especificadas estiverem habilitadas para proteção contra encerramento, a solicitação apresentará os seguintes resultados de falha:

- As instâncias especificadas que estão na mesma zona de disponibilidade que a instância protegida não estão terminadas.
- As instâncias especificadas que estão em zonas de disponibilidade diferentes, em que nenhuma outra instância especificada está protegida, estão terminadas corretamente.

Por exemplo, digamos que você tenha as seguintes instâncias:

Instância	Availability Zone	Encerrar proteção
Instância A	us-east-1a	Disabled
Instância B		Disabled
Instância C	us-east-1b	Enabled
Instância D		Disabled

Se você tentar terminar todas essas instâncias na mesma solicitação, a solicitação relatará falha com os seguintes resultados:

- Instância A e Instância B estão terminadas corretamente porque nenhuma das instâncias especificadas em us-east-1a está habilitada para proteção contra término.
- Instância C e Instância D não conseguem terminar porque pelo menos uma das instâncias especificadas em us-east-1b (Instância C) está habilitada para proteção contra término.

O que acontece quando você encerra uma instância

Quando uma instância do EC2 é encerrada usando o comando `terminate-instances`, o seguinte é registrado no nível do SO:

- A solicitação da API enviará um evento de pressionamento de botão ao convidado.
- Vários serviços do sistema serão interrompidos como resultado do evento de pressionamento do botão. O `systemd` executa um desligamento normal do sistema. O desligamento normal é acionado pelo evento de pressionamento do botão de desligamento de ACPI do hipervisor.
- O desligamento de ACPI será iniciado.
- A instância será desligada quando o processo de desligamento normal terminar. Não existe um tempo de desligamento configurável para o SO.

Como encerrar uma instância

Você pode encerrar uma instância usando o AWS Management Console ou a linha de comando.

Por padrão, ao iniciar a desativação de uma instância baseada em Amazon EBS (usando os comandos shutdown ou poweroff), a instância será interrompida. O comando halt não inicia um desligamento. Se ele for usado, a instância não será encerrada. Em vez disso, ele colocará a CPU em HALT e a instância permanecerá em execução.

New console

Para encerrar uma instância usando o console

1. Antes de encerrar a instância, confirme que não perderá dados verificando se seus volumes do Amazon EBS não serão excluídos no encerramento e se você copiou todos os dados de que precisa dos volumes de armazenamento persistente de instância, como o Amazon EBS ou o Amazon S3.
2. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
3. No painel de navegação, escolha Instances (Instâncias).
4. Selecione a instância e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).
5. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Old console

Para encerrar uma instância usando o console

1. Antes de encerrar a instância, confirme que não perderá dados verificando se seus volumes do Amazon EBS não serão excluídos no encerramento e se você copiou todos os dados de que precisa dos volumes de armazenamento persistente de instância, como o Amazon EBS ou o Amazon S3.
2. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
3. No painel de navegação, escolha Instances (Instâncias).
4. Selecione a instância e escolha Actions, Instance State e Terminate.
5. Quando a confirmação for solicitada, escolha Sim, encerrar.

Para encerrar uma instância usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [terminate-instances](#) (AWS CLI)
- [Stop-EC2Instance](#) (AWS Tools for Windows PowerShell)

Habilitar a proteção contra encerramento

Por padrão, você pode encerrar sua instância usando o console do Amazon EC2, a interface de linha de comando ou a API. Se você quiser impedir que sua instância seja interrompida accidentalmente usando o Amazon EC2, pode habilitar a proteção contra a interrupção da instância. O atributo DisableApiTermination define se a instância pode ser encerrada usando o console, a CLI ou a API. Por padrão, a proteção contra encerramento está desabilitada para sua instância. Você pode definir o valor desse atributo ao executar a instância, enquanto a instância estiver em execução ou quando a instância for interrompida (para instâncias baseadas no Amazon EBS).

O atributo `DisableApiTermination` não impede que você encerre uma instância iniciando o desligamento da instância (usando um comando do sistema operacional para o desligamento do sistema) quando o atributo `InstanceStateInitiatedShutdownBehavior` é definido. Para obter mais informações, consulte [Alterar o comportamento de desligamento iniciado da instância \(p. 477\)](#).

Limitations

Não é possível habilitar a proteção contra encerramento para uma instância spot. Uma instância spot é encerrada quando o preço spot excede o valor que você está disposto a pagar por instâncias spot. No entanto, é possível preparar sua aplicação para lidar com interrupções de instância spot. Para obter mais informações, consulte [Interrupções de instâncias spot \(p. 336\)](#).

O atributo `DisableApiTermination` não impede que o Amazon EC2 Auto Scaling encerre uma instância. Para instâncias em um grupo do Auto Scaling, use os seguintes recursos do Amazon EC2 Auto Scaling em vez de a proteção contra encerramento do Amazon EC2:

- Para impedir que as instâncias que fazem parte de um grupo do Auto Scaling sejam encerradas na redução, use a proteção da instância. Para obter mais informações, consulte [Proteção de instâncias](#) no Guia do usuário do Amazon EC2 Auto Scaling.
- Para impedir que o Amazon EC2 Auto Scaling encerre instâncias não íntegras, suspenda o processo `ReplaceUnhealthy`. Para obter mais informações, consulte [Suspensão e retomada dos processos de escalabilidade](#) no Guia do usuário do Amazon EC2 Auto Scaling.
- Para especificar quais instâncias do Amazon EC2 Auto Scaling devem ser encerradas primeiro, escolha uma política de encerramento. Para obter mais informações, consulte [Personalização da política de encerramento](#) no Guia do usuário do Amazon EC2 Auto Scaling.

Para habilitar a proteção contra encerramento de uma instância no momento da execução

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel, escolha Launch Instance (Executar instância) e siga as instruções contidas no assistente.
3. Na página Configure Instance Details (Configurar detalhes da instância), marque a caixa de seleção `Enable termination protection` (Habilitar proteção contra encerramento).

Para habilitar a proteção contra encerramento de uma instância em execução ou interrompida

1. Selecione a instância, escolha Actions (Ações), Instance Settings (Configurações da instância) e selecione Change Termination Protection (Alterar proteção contra interrupção).
2. Escolha Yes, Enable (Sim, habilitar).

Para desabilitar a proteção contra encerramento de uma instância em execução ou interrompida

1. Selecione a instância, escolha Actions (Ações), Instance Settings (Configurações da instância) e selecione Change Termination Protection (Alterar proteção contra interrupção).
2. Escolha Yes, Disable (Sim, desabilitar).

Para habilitar ou desabilitar a proteção contra encerramento usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

Alterar o comportamento de desligamento iniciado da instância

Por padrão, quando você inicia um desligamento em uma instância baseada no Amazon EBS (usando um comando como shutdown ou poweroff), a instância é interrompida (observe que halt não emite um

comando poweroff e, se usado, a instância não será encerrada. Em vez disso, ela colocará a CPU em HLT e a instância permanecerá em execução). Você pode alterar esse comportamento usando o atributo `InstanceInitiatedShutdownBehavior` para a instância de forma que, em vez de ser desligada, ela seja encerrada. Você pode atualizar esse atributo enquanto a instância estiver sendo executada ou interrompida.

Você pode atualizar o atributo `InstanceInitiatedShutdownBehavior` usando o console do Amazon EC2 ou a linha de comando. O atributo `InstanceInitiatedShutdownBehavior` se aplica apenas quando você executa uma desativação do sistema operacional da própria instância; ele não se aplica quando você interrompe uma instância usando a API `StopInstances` ou o console do Amazon EC2.

Para alterar o comportamento de desligamento de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Escolha Actions (Ações), Instance settings (Configurações da instância), Change shutdown behavior (Alterar comportamento de desativação). O comportamento atual é selecionado.
5. Para alterar o comportamento, selecione Stop (Interromper) ou Terminate (Encerrar) em Shutdown behavior (Comportamento de desativação) e escolha Apply (Aplicar).

Para alterar o comportamento de desligamento de uma instância usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- `modify-instance-attribute` (AWS CLI)
- `Edit-EC2InstanceAttribute` (AWS Tools for Windows PowerShell)

Preservar volumes do Amazon EBS no encerramento da instância

Quando uma instância é encerrada, o Amazon EC2 usa o valor do atributo `DeleteOnTermination` para cada volume do Amazon EBS anexado a fim de determinar se o volume será preservado ou excluído.

O valor padrão do atributo `DeleteOnTermination` difere dependendo de se o volume é o volume raiz da instância ou um volume não raiz anexado à instância.

Volume raiz

Por padrão, o atributo `DeleteOnTermination` para o volume raiz de uma instância é definido como `true`. Portanto, o padrão é excluir o volume raiz da instância quando a instância é encerrada. O atributo `DeleteOnTermination` pode ser definido pelo criador de uma AMI, bem como pela pessoa que executa a instância. Quando o atributo é alterado pelo criador de uma AMI ou pela pessoa que executa uma instância, a nova configuração substitui a configuração padrão original da AMI. Recomendamos que você verifique a configuração padrão do atributo `DeleteOnTermination` após executar uma instância com uma AMI.

Volume não raiz

Por padrão, ao [anexar um volume do EBS não raiz a uma instância \(p. 1271\)](#), seu atributo `DeleteOnTermination` é definido como `false`. Portanto, o padrão é preservar esses volumes. Depois que a instância é encerrada, você pode criar uma snapshot do volume preservado ou anexá-lo a outra instância. Exclua um volume para evitar cobranças adicionais. Para obter mais informações, consulte [Excluir um volume de Amazon EBS \(p. 1293\)](#).

Para verificar o valor do atributo `DeleteOnTermination` de um volume do EBS que esteja em uso, consulte o mapeamento de dispositivos de bloco da instância. Para obter mais informações, consulte [Visualizar os volumes do EBS em um mapeamento de dispositivos de blocos de instância \(p. 1522\)](#).

Você pode alterar o valor do atributo `DeleteOnTermination` de um volume quando executar a instância ou enquanto a instância estiver sendo executada.

Exemplos

- [Alterar o volume raiz a ser mantido na execução usando o console \(p. 479\)](#)
- [Alterar o volume raiz a ser mantido na execução usando a linha de comando \(p. 479\)](#)
- [Alterar o volume raiz de uma instância em execução a ser mantido usando a linha de comando \(p. 480\)](#)

Alterar o volume raiz a ser mantido na execução usando o console

Usando o console, você pode alterar o atributo `DeleteOnTermination` quando executar uma instância. Para alterar esse atributo para uma instância em execução, use a linha de comando.

Para alterar o volume raiz de uma instância a ser mantido na execução usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel do console, selecione Launch Instance (Executar instância).
3. Na página Choose an Amazon Machine Image (AMI) (Escolher uma imagem de máquina da Amazon), selecione uma AMI e escolha Select (Selecionar).
4. Siga o assistente para preencher as páginas Choose an Instance Type e Configure Instance Details.
5. Na página Add Storage, desmarque a caixa de seleção Delete On Termination do volume do dispositivo raiz.
6. Preencha as páginas restantes do assistente e escolha Launch (Executar).

Na nova experiência do console, você pode verificar a configuração exibindo detalhes do volume raiz do dispositivo no painel de detalhes da instância. Na guia Armazenamento, em Dispositivos de blocos, role para a direita para ver a configuração Excluir no encerramento para o volume. Por padrão, Delete on termination é Yes. Se você alterar o comportamento padrão, Delete on termination será No.

Na experiência antiga do console, você pode verificar a configuração exibindo detalhes do volume raiz do dispositivo no painel de detalhes da instância. Ao lado de Dispositivos de blocos, selecione a entrada do volume do dispositivo raiz. Por padrão, Delete on termination é True. Se você alterar o comportamento padrão, Delete on termination será False.

Alterar o volume raiz a ser mantido na execução usando a linha de comando

Ao executar uma instância baseada no EBS, você pode usar um dos seguintes comandos para alterar o volume do dispositivo raiz a ser mantido. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [run-instances](#) (AWS CLI)
- [New-EC2Instance](#) (AWS Tools for Windows PowerShell)

Por exemplo, adicione a opção a seguir ao seu comando `run-instances`:

```
--block-device-mappings file:/mapping.json
```

Especifique o seguinte em `mapping.json`:

```
[  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "DeleteOnTermination": false,  
      "SnapshotId": "snap-1234567890abcdef0",  
      "VolumeType": "gp2"  
    }  
  }  
]
```

Alterar o volume raiz de uma instância em execução a ser mantido usando a linha de comando

Você pode usar um dos seguintes comandos para alterar o volume do dispositivo raiz de uma instância baseada no EBS em execução a ser mantido. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

Por exemplo, use o comando a seguir:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings  
file://mapping.json
```

Especifique o seguinte em `mapping.json`:

```
[  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "DeleteOnTermination": false  
    }  
  }  
]
```

Recuperar a instância

Você pode criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2 e recupere-a automaticamente se ocorrer um problema devido a uma falha de hardware subjacente ou um problema que exija o envolvimento da AWS para repará-lo. Instâncias encerradas não podem ser recuperadas.

Uma instância recuperada é idêntica à instância original, incluindo o ID da instância, endereços IP privados, endereços IP elásticos e todos os metadados de instância. Se a instância prejudicada tiver um endereço IPv4 público, ela referá esse endereço após a recuperação. Se a instância danificada estiver em um placement group, a instância recuperada será executada no placement group.

Quando o alarme `StatusCheckFailed_System` for acionado, e a ação de recuperação for iniciada, você será notificado pelo tópico do Amazon SNS que você selecionou ao criar o alarme e a ação de recuperação associada. Durante a recuperação da instância, a instância será migrada durante uma reinicialização da instância e todos os dados na memória serão perdidos. Quando o processo é concluído,

as informações serão publicadas no tópico do SNS que você tiver configurado para o alarme. Qualquer pessoa que estiver inscrita neste tópico do SNS receberá uma notificação por e-mail com o status da tentativa de recuperação e mais instruções. Você perceberá uma reinicialização da instância na instância recuperada.

Exemplos de problemas que causam falha nas verificações de status do sistema incluem:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de software no host físico
- Problemas de hardware de host físico que afetam a acessibilidade de rede

Tópicos

- [Requirements \(p. 481\)](#)
- [Crie um alarme Amazon CloudWatch para recuperar uma instância \(p. 481\)](#)
- [Solucionar problemas de falhas de recuperação da instância \(p. 481\)](#)

Requirements

A ação de recuperação é compatível somente nas instâncias com as seguintes características:

- Usa um dos seguintes tipos de instância: C3, C4, C5, C5a, C5n, M3, M4, M5, M5a, M5n, M5zn, M6i, P3, R3, R4, R5, R5a, R5b, R5n, T2, T3, T3a, alta memória (apenas virtualizada), X1, X1e
- Executa em uma nuvem privada virtual (VPC)
- O default ou locação da instância dedicated
- Tem apenas volumes do EBS (não configure volumes de armazenamento de instâncias).

Crie um alarme Amazon CloudWatch para recuperar uma instância

Para obter informações sobre como criar um Amazon CloudWatch alarme para recuperar uma instância, consulte [Adicionar ações de recuperação a alarmes do Amazon CloudWatch \(p. 930\)](#).

Solucionar problemas de falhas de recuperação da instância

Os problemas a seguir podem fazer com que a recuperação automática da sua instância falhe:

- Capacidade temporária e insuficiente do hardware de substituição.
- A instância tem um armazenamento de instâncias associado, para o qual não há configuração compatível com recuperação automática da instância.
- Há um evento em andamento no Service Health Dashboard que impediu a execução bem-sucedida do processo de recuperação. Consulte <http://status.aws.amazon.com/> para obter as informações mais recentes sobre disponibilidade do serviço.
- A instância alcançou a franquia diária máxima de três tentativas de recuperação.

O processo de recuperação automática tentará recuperar sua instância por até três falhas separadas por dia. Se a falha de verificação de status do sistema da instância persistir, recomendamos que você pare e inicie manualmente a instância. Para obter mais informações, consulte [Interromper e iniciar sua instância \(p. 455\)](#).

Sua instância poderá ser subsequentemente aposentada se recuperação automática falhar e determinar-se que a degradação de hardware é a causa-raiz da falha de verificação do status do sistema original.

Configurar sua instância do Windows

Uma instância Windows é um servidor virtual que executa o Windows Server na nuvem.

Depois de executar e fazer login na sua instância com êxito, você pode fazer alterações nela para configurá-la a fim de atender às necessidades de uma aplicação específica. A seguir, temos algumas tarefas comuns para ajudar você a começar.

Tópicos

- [Configurar uma instância do Windows usando o EC2Launch v2 \(p. 482\)](#)
- [Configurar uma instância do Windows usando o EC2Launch \(p. 522\)](#)
- [Configurar uma instância do Windows usando o serviço EC2Config \(p. 530\)](#)
- [Drivers paravirtuais para as instâncias do Windows \(p. 559\)](#)
- [AWSDrivers NVMe para instâncias do Windows \(p. 580\)](#)
- [Otimizar as opções de CPU \(p. 582\)](#)
- [Definir o horário para uma instância do Windows. \(p. 601\)](#)
- [Definir a senha para uma instância do Windows \(p. 605\)](#)
- [Adicionar componentes do Windows usando mídia de instalação \(p. 606\)](#)
- [Configurar um endereço IPv4 privado secundário para uma instância do Windows. \(p. 610\)](#)
- [Executar comandos na instância do Windows na inicialização \(p. 614\)](#)
- [Metadados da instância e dados do usuário \(p. 622\)](#)
- [Melhores práticas e recomendações para o clustering do SQL Server no EC2 \(p. 670\)](#)

Configurar uma instância do Windows usando o EC2Launch v2

Todas as instâncias compatíveis do Amazon EC2 que executam o Windows Server incluem o agente de inicialização do EC2Launch v2 (`EC2Launch.exe`). O EC2Launch v2 executa tarefas durante o startup da instância e é executado se uma instância for interrompida e iniciada posteriormente, ou reiniciada. O EC2Launch v2 também pode executar tarefas sob demanda. Algumas dessas tarefas são automaticamente habilitadas, enquanto outras precisam ser habilitadas manualmente. O serviço EC2Launch v2 é compatível com todos os recursos EC2Config e EC2Launch.

Esse serviço usa um arquivo de configuração para controlar sua operação. Você pode atualizar o arquivo de configuração usando uma ferramenta gráfica ou editando-o diretamente como único arquivo `.yml` (`agent-config.yml`). Os binários de serviço ficam localizados no diretório `%ProgramFiles%\Amazon\EC2Launch`.

O EC2Launch v2 publica logs de eventos do Windows para ajudá-lo a solucionar erros e definir gatilhos. Para obter mais informações, consulte [Logs de eventos do Windows \(p. 515\)](#).

Sistemas operacionais com suporte

- Windows Server 2022
- Windows Server 2019 (canal de manutenção de longo prazo e canal semestral)

- Windows Server 2016
- Windows Server 2012 e 2012 R2
- Windows Server 2008 SP2 e 2008 R2

Conteúdos da seção EC2Launch v2

- [Visão geral do EC2Launch v2 \(p. 483\)](#)
- [Instalar a versão mais recente do EC2Launch v2 \(p. 487\)](#)
- [Migrar para o EC2Launch v2 \(p. 488\)](#)
- [Interromper, reiniciar, excluir ou desinstalar o EC2Launch v2 \(p. 489\)](#)
- [Verificar a versão do EC2Launch v2 \(p. 490\)](#)
- [Assinar notificações do serviço EC2Launch v2 \(p. 491\)](#)
- [Configurações do EC2Launch v2 \(p. 491\)](#)
- [Soluç�ao de problemas do EC2Launch v2 \(p. 513\)](#)
- [Históricos de versões do EC2Launch v2 \(p. 520\)](#)

Visão geral do EC2Launch v2

O EC2Launch v2 é um serviço que executa tarefas durante o startup da instância e é executado se uma instância for interrompida e iniciada posteriormente, ou reiniciada.

Tópicos de visão geral

- [Comparar serviços de inicialização do Amazon EC2 \(p. 483\)](#)
- [Conceitos do EC2Launch v2 \(p. 484\)](#)
- [Tarefas do EC2Launch v2 \(p. 485\)](#)
- [Telemetry \(p. 486\)](#)

Comparar serviços de inicialização do Amazon EC2

A tabela a seguir mostra as principais diferenças funcionais entre EC2Config, EC2Launch v1 e EC2Launch v2.

Recurso	EC2Config	EC2Launch v1	EC2Launch v2
Executado como	Windows Service	Scripts PowerShell	Windows Service
Supporte	Windows 2003 Windows 2008 Windows 2008 R2 Windows 2012 Windows 2012 R2	Windows 2016 Windows 2019 (LTSC e SAC)	Windows 2008 Windows 2008 R2 Windows 2012 Windows 2012 R2 Windows 2016 Windows 2019 (LTSC e SAC) Windows 2022

Recurso	EC2Config	EC2Launch v1	EC2Launch v2
Arquivo de configuração	XML	XML	YAML
Definir nome de usuário do administrador	Não	Não	Sim
Tamanho dos dados do usuário	16 KB	16 KB	60 KB (compactado)
Dados de usuário local incorporados na AMI	Não	Não	Sim, configurável
Configuração de tarefa nos dados do usuário	Não	Não	Sim
Papel de parede configurável	Não	Não	Sim
Personalizar ordem de execução da tarefa	Não	Não	Sim
Tarefas configuráveis	15	9	20 na execução
Oferece suporte ao Visualizador de eventos do Windows	Sim	Não	Sim
Número dos tipos de eventos do Visualizador de eventos	2	0	30

Conceitos do EC2Launch v2

É útil entender os conceitos a seguir ao considerar o EC2Launch v2.

Task

Uma tarefa pode ser invocada para execução de uma ação em uma instância. Para obter uma lista completa das tarefas disponíveis do EC2Launch v2, consulte [Tarefas do EC2Launch v2 \(p. 485\)](#). Cada tarefa inclui um conjunto de estágios nos quais pode ser executada, uma frequência definida e entradas. As tarefas podem ser configuradas no arquivo `agent-config` ou por meio de `user-data`.

Stages

Um estágio é um agrupamento lógico de tarefas executadas pelo serviço. Algumas tarefas podem ser executadas apenas em um estágio específico. Outras podem ser executadas em vários estágios. Ao usar dados locais, você deve especificar o estágio em que uma tarefa será executada. Ao usar dados do usuário, o estágio é implícito.

A lista a seguir mostra os estágios na ordem em que são executados:

1. Inicialização
2. Rede
3. PreReady
4. PostReady
5. UserData

Frequency

A frequência da tarefa é usada para agendar quando as tarefas devem ser executadas de acordo com o contexto de inicialização.

As seguintes frequências podem ser especificadas:

- Uma vez — a tarefa é executada uma vez, mediante a inicialização da AMI pela primeira vez (Sysprep concluído).
- Sempre — a tarefa é executada toda vez que o agente de inicialização é executado. O agente de inicialização é executado quando:
 - uma instância inicia ou reinicia
 - o serviço EC2Launch é executado
 - `EC2Launch.exe runO` é invocado

agent-config

O `agent-config` é um arquivo localizado na pasta de configuração do EC2Launch v2. Ele inclui configuração para os estágios de inicialização, rede, antes de pronto e depois de pronto. Este arquivo é usado para especificar a configuração de uma instância para tarefas que devem ser executadas quando a AMI é inicializada pela primeira vez ou para horários subsequentes.

Por padrão, a instalação do EC2Launch v2 instala um arquivo `agent-config` que inclui configurações recomendadas usadas nas AMIs padrão do Amazon Windows. Você pode atualizar o arquivo de configuração de modo a alterar a experiência de inicialização padrão para sua AMI especificada pelo EC2Launch v2.

Dados do usuário

Os dados do usuário são dados que podem ser configurados ao iniciar uma instância. Você pode atualizar os dados do usuário para alterar de maneira dinâmica como as AMIs personalizadas ou AMIs de início rápido são configuradas. O EC2Launch v2 suporta 60 kB de comprimento de entrada de dados do usuário. Os dados do usuário incluem apenas o estágio do UserData e, portanto, são executados após o arquivo `agent-config`. Você pode inserir dados do usuário ao executar uma instância usando o assistente de execução de instância ou pode modificar os dados do usuário no console do EC2. Para obter mais informações sobre como trabalhar com dados do usuário, consulte [Executar comandos na instância do Windows na inicialização \(p. 614\)](#).

Tarefas do EC2Launch v2

O EC2Launch v2 pode executar as seguintes tarefas em cada inicialização:

- Configurar papel de parede novo e opcionalmente personalizado que renderiza informações sobre a instância.
- Definir os atributos para a conta de administrador criada na máquina local.
- Adicionar sufixos DNS à lista de sufixos de pesquisa. Somente sufixos que ainda não existem são adicionados à lista.
- Definir letras de unidade para quaisquer volumes adicionais e estendê-las para usar o espaço disponível.
- Gravar arquivos no disco, seja da Internet ou da configuração. Se o conteúdo estiver na configuração, ele pode ser decodificado ou codificado em base64. Se o conteúdo for da internet, ele pode ser descompactado.
- Executar scripts da Internet ou da configuração. Se o script for da configuração, ele pode ser decodificado em base64. Se o script for da internet, ele pode ser descompactado.

- Executar um programa com os argumentos fornecidos.
- Definir o nome do computador.
- Enviar informações de instância para o console do Amazon EC2.
- Enviar a impressão digital do certificado RDP ao console do EC2.
- Estenda dinamicamente a partição do sistema operacional para incluir qualquer espaço não particionado.
- Executar dados do usuário. Para obter mais informações sobre como especificar os dados do usuário, consulte [Configuração de tarefas do EC2Launch v2 \(p. 503\)](#).
- Definir rotas estáticas persistentes para alcançar o serviço de metadados e os servidores AWS KMS.
- Definir partições não inicializáveis como MBR ou GPT.
- Iniciar o serviço Systems Manager (SSM) após o Sysprep.
- Otimizar as configurações do ENA.
- Ativar o OpenSSH para versões posteriores do Windows.
- Ativar os frames jumbo.
- Defina o Sysprep para execução com o EC2Launch v2.
- Publicar logs de eventos do Windows.

Telemetry

Telemetria é informação adicional que ajuda o AWS a entender melhor suas necessidades, diagnosticar problemas e fornecer recursos para melhorar sua experiência com os serviços da AWS.

EC2Launch versão v2 2 . 0 . 592 e, posteriormente, coletar telemetria, como métricas de uso e erros. Esses dados são coletados da instância do Amazon EC2 na qual o EC2Launch v2 é executado. Isso inclui todas as AMIs do Windows de propriedade da AWS.

Os seguintes tipos de telemetria são coletados pelo EC2Launch v2:

- Informações de uso: comandos do agente, método de instalação e frequência de execução programada.
- Erros e informações de diagnóstico: instalação do agente e execução dos códigos de erro.

Exemplos de dados coletados pelo:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

A telemetria está habilitada por padrão. Você pode desativar a coleta de telemetria a qualquer momento. Se a telemetria estiver ativada, o EC2Launch v2 enviará dados de telemetria sem notificações adicionais do cliente.

Visibilidade de telemetria

Quando a telemetria é ativada, ela aparece na saída do console do Amazon EC2 da seguinte maneira:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Desativar telemetria em uma instância

Para desativar a telemetria para uma única instância, você pode definir uma variável de ambiente do sistema ou usar o MSI para modificar a instalação.

Para desativar a telemetria definindo uma variável de ambiente do sistema, execute o seguinte comando como administrador:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Para desabilitar a telemetria usando o MSI, execute o seguinte comando depois de [baixar o MSI \(p. 487\)](#):

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Instalar a versão mais recente do EC2Launch v2

O EC2Launch v2 está disponível atualmente por download, instalação do Distribuidor SSM e em todas as AMIs compatíveis do Windows.

Download

Para instalar a versão mais recente do EC2Launch v2, faça download do serviço dos seguintes locais:

Note

O AmazonEC2Launch.msi não desinstala versões anteriores dos serviços de inicialização do EC2, como o EC2Launch (v1) ou o EC2Config. A fim de atualizar para o EC2Launch v2 de uma versão anterior do serviço de inicialização, consulte [Migrar para o EC2Launch v2 \(p. 488\)](#).

- 64 bits — <https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi>
- 32 bits — <https://s3.amazonaws.com/amazon-ec2launch-v2/windows/386/latest/AmazonEC2Launch.msi>

Instalar do Distribuidor SSM da AWS

Você pode instalar o pacote AWSEC2Launch-Agent do Distribuidor SSM da AWS. Para obter instruções sobre como instalar um pacote do Distribuidor SSM, consulte [Install or update packages \(Instalar ou atualizar pacotes\)](#) no AWS SSM User Guide (Manual do usuário do AWS SSM).

Usar a AMI com EC2Launch v2 pré-instalado (workloads que não sejam de produção)

O EC2Launch v2 está pré-instalado nas AMIs a seguir. Não use essas AMIs para workloads de produção, pois elas se destinam somente a verificar se o serviço do funciona bem com os processos e workloads existentes. Você pode [encontrar essas AMIs no console do Amazon EC2](#) ou [usando a CLI do EC2](#) e pesquisando com o prefixo EC2LaunchV2_Preview-Windows_Server-.

- EC2LaunchV2_Preview-Windows_Server-2004-English-Core-Base
- EC2LaunchV2_Preview-Windows_Server-2019-English-Full-Base
- EC2LaunchV2_Preview-Windows_Server-2019-English-Core-Base
- EC2LaunchV2_Preview-Windows_Server-2016-English-Full-Base
- EC2LaunchV2_Preview-Windows_Server-2016-English-Core-Base
- EC2LaunchV2_Preview-Windows_Server-2012_R2_RTM-English-Full-Base
- EC2LaunchV2_Preview-Windows_Server-2012_R2_RTM-English-Core
- EC2LaunchV2_Preview-Windows_Server-2012_RTM-English-Full-Base
- EC2LaunchV2_Preview-Windows_Server-2019-English-Full-SQL_2019_Express

- EC2LaunchV2_Preview-Windows-Server-2016-English-Full-SQL_2017_Express

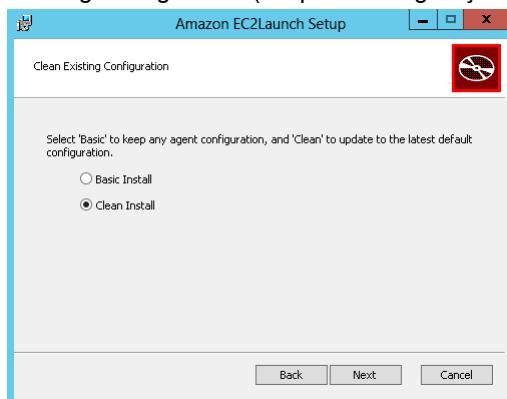
Opções de instalação

Quando você instala ou atualiza o EC2Launch v2, a sua configuração existente, localizada em %ProgramData%/Amazon/EC2Launch/config/agent-config.yml, não é substituída. Execute uma instalação limpa para substituir uma configuração existente para usar a versão mais recente.

Você pode executar uma instalação limpa usando a interface ou a linha de comando do EC2Launch v2.

Executar uma instalação limpa usando a interface do usuário do EC2Launch v2

Quando você instalar o EC2Launch v2, escolha a opção Clean Install (Instalação limpa) abaixo de Clean Existing Configuration (Limpar a configuração existente).



Execute uma instalação limpa usando a linha de comando

Para executar uma instalação limpa do EC2Launch v2 usando a linha de comando, execute o seguinte comando do Windows:

```
msiexec /i "C:\Users\Administrator\Desktop\AmazonEC2Launch.msi" ADDLOCAL="Basic,Clean" /q
```

Migrar para o EC2Launch v2

A ferramenta de migração do EC2Launch atualiza o agente de inicialização instalado (EC2Config e EC2Launch v1) ao desinstalá-lo e ao instalar o EC2Launch v2. As configurações aplicáveis dos serviços de inicialização anteriores são migradas automaticamente para o novo serviço. A ferramenta de migração não detecta qualquer tarefa agendada vinculada aos scripts do EC2Launch v1; portanto, ela não configura automaticamente essas tarefas no EC2Launch v2. Para configurar essas tarefas, edite o arquivo [agent-config.yml \(p. 503\)](#) ou use a [caixa de diálogo de configurações do EC2Launch v2 \(p. 491\)](#). Por exemplo, se uma instância tiver uma tarefa agendada que executa `InitializeDisks.ps1`, depois de executar a ferramenta de migração, você deverá especificar os volumes que deseja inicializar na caixa de diálogo de configurações do EC2Launch v2. Consulte a Etapa 6 do procedimento para [Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2 \(p. 491\)](#).

Você pode baixar a ferramenta de migração ou instalar com um documento SSM RunCommand.

Você pode fazer download da ferramenta nos seguintes locais.

- 64 bits — <https://s3.amazonaws.com/amazon-ec2launch-v2-utils/MigrationTool/windows/amd64/latest/EC2LaunchMigrationTool.zip>
- 32 bits — <https://s3.amazonaws.com/amazon-ec2launch-v2-utils/MigrationTool/windows/386/latest/EC2LaunchMigrationTool.zip>

Note

É necessário executar a ferramenta de migração do EC2Launch v2 como administrador. O EC2Launch v2 é instalado como um serviço depois da execução da ferramenta de migração. Ele não é executado imediatamente. Por padrão, ele é executado durante o startup da instância e é executado se uma instância for interrompida e posteriormente iniciada ou reiniciada.

Use o documento do SSM [AWSEC2Launch-RunMigration](#) para migrar para a versão mais recente do EC2Launch com o Run Command do SSM. O documento não requer parâmetros. Para obter mais informações sobre como usar o Run Command do SSM, consulte [AWS Systems Manager Run Command \(Run Command do AWS Systems Manager\)](#).

A ferramenta de migração aplica as configurações a seguir do EC2Config ao EC2Launch v2.

- Se `Ec2DynamicBootVolumeSize` for definido como `false`, o EC2Launch v2 será removido da etapa `boot`
- Se `Ec2SetPassword` estiver definido como `Enabled`, o tipo de senha do EC2Launch v2 será definido como `random`
- Se `Ec2SetPassword` estiver definido como `Disabled`, o tipo de senha do EC2Launch v2 será definido como `donothing`
- Se `SetDnsSuffixList` for definido como `false`, o EC2Launch v2 será removido da tarefa `setDnsSuffix`
- Se `EC2SetComputerName` estiver definido como verdadeiro, a tarefa `setHostName` do EC2Launch v2 será adicionada à configuração do `yaml`

A ferramenta de migração aplica as configurações a seguir do EC2Launch v1 ao EC2Launch v2.

- Se `ExtendBootVolumeSize` for definido como `false`, o EC2Launch v2 será removido da etapa `boot`
- Se `AdminPasswordType` estiver definido como `Random`, o tipo de senha do EC2Launch v2 será definido como `random`
- Se `AdminPasswordType` estiver definido como `Specify`, o tipo de senha do EC2Launch v2 será definido como `static` e os dados da senha como a senha especificada em `AdminPassword`
- Se `SetWallpaper` for definido como `false`, o EC2Launch v2 será removido da tarefa `setWallpaper`
- Se `AddDnsSuffixList` for definido como `false`, o EC2Launch v2 será removido da tarefa `setDnsSuffix`
- Se `SetComputerName` for definido como `true`, a tarefa `setHostName` do EC2Launch v2 será adicionada

Interromper, reiniciar, excluir ou desinstalar o EC2Launch v2

Você pode gerenciar o serviço EC2Launch v2 da mesma forma como qualquer outro serviço do Windows.

O EC2Launch v2 é executado uma vez na inicialização e executa todas as tarefas configuradas. Depois de executar as tarefas, o serviço entra no estado interrompido. Quando você reinicia o serviço, ele executa todas as tarefas configuradas novamente e retorna ao estado interrompido.

Para aplicar as configurações atualizadas à sua instância, interrompa e reinicie o serviço. Se estiver instalando manualmente o EC2Launch v2, você deverá interromper o serviço primeiro.

Para interromper o serviço EC2Launch v2

1. Execute e conecte-se à sua instância do Windows.

2. No menu Iniciar, selecione Ferramentas Administrativas e abra Serviços.
3. Na lista de serviços, clique com o botão direito sobre Amazon EC2Launch e selecione Parar.

Para reiniciar o serviço EC2Launch v2

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, selecione Ferramentas Administrativas e abra Serviços.
3. Na lista de serviços, clique com o botão direito sobre Amazon EC2Launch e selecione Reiniciar.

Se não precisar atualizar as configurações, ao criar sua própria AMI ou usar o AWS Systems Manager, você poderá excluir e desinstalar de serviço. A exclusão de um serviço remove a subchave do registro. Desinstalar um serviço elimina os arquivos, as subchaves do registro e todos os atalhos do serviço.

Para excluir o serviço EC2Launch v2

1. Inicie uma janela do prompt de comando.
2. Execute o seguinte comando:

```
sc delete EC2Launch
```

Para desinstalar o EC2Launch v2

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, selecione Painel de Controle.
3. Abra Programas e Recursos.
4. Na lista de programas, selecione Amazon EC2Launch v2 e Desinstalar.

Verificar a versão do EC2Launch v2

Use o procedimento a seguir para verificar a versão do EC2Launch v2 que está instalada nas suas instâncias.

Para verificar a versão instalada do EC2Launch v2

1. Execute uma instância pela AMI e conecte-se a ela.
2. No Painel de Controle, selecione Programs and Features (Programas e recursos).
3. Na lista de programas instalados, procure Amazon EC2Launch. O número da versão aparece na coluna Versão.

Para obter mais informações sobre as versões do EC2Launch incluídas nas AMIs do Windows, consulte [AWSAMIs do Windows \(p. 29\)](#).

Para obter a versão mais recente do EC2Launch v2, consulte [Histórico de versões do EC2Launch v2 \(p. 520\)](#).

Para obter a versão mais recente da ferramenta de migração do EC2Launch v2, consulte [Histórico de versões da ferramenta de migração do EC2Launch v2 \(p. 521\)](#).

Você pode receber notificações quando novas versões do serviço EC2Launch v2 forem liberadas. Para obter mais informações, consulte [Assinar notificações do serviço EC2Launch v2 \(p. 491\)](#).

Assinar notificações do serviço EC2Launch v2

O Amazon SNS pode notificá-lo quando novas versões do serviço EC2Launch v2 forem liberadas. Use o procedimento a seguir para se inscrever nessas notificações.

Assinar notificações do EC2Launch v2

1. Faça login no AWS Management Console e abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. Você deve selecionar esta Região porque as notificações do SNS que você está assinando foram criadas nesta Região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
 - a. Para ARN do tópico, use o seguinte Nome de recurso da Amazon (ARN): arn:aws:sns:us-east-1:309726204594:amazon-ec2launch-v2.
 - b. Em Protocol (Protocolo), escolha Email.
 - c. Em Endpoint, insira um endereço de e-mail que possa ser usado para receber notificações.
 - d. Selecione Create subscription.
6. Você receberá um e-mail solicitando a confirmação de sua assinatura. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que uma nova versão do serviço EC2Launch v2 for liberada, nós enviaremos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

1. Abra o console do Amazon SNS.
2. No painel de navegação, escolha Subscriptions.
3. Selecione a assinatura e escolha Actions (Ações), Delete subscriptions (Excluir assinaturas). Quando a confirmação for solicitada, escolha Excluir.

Configurações do EC2Launch v2

Esta seção contém informações sobre como definir configurações para o EC2Launch v2.

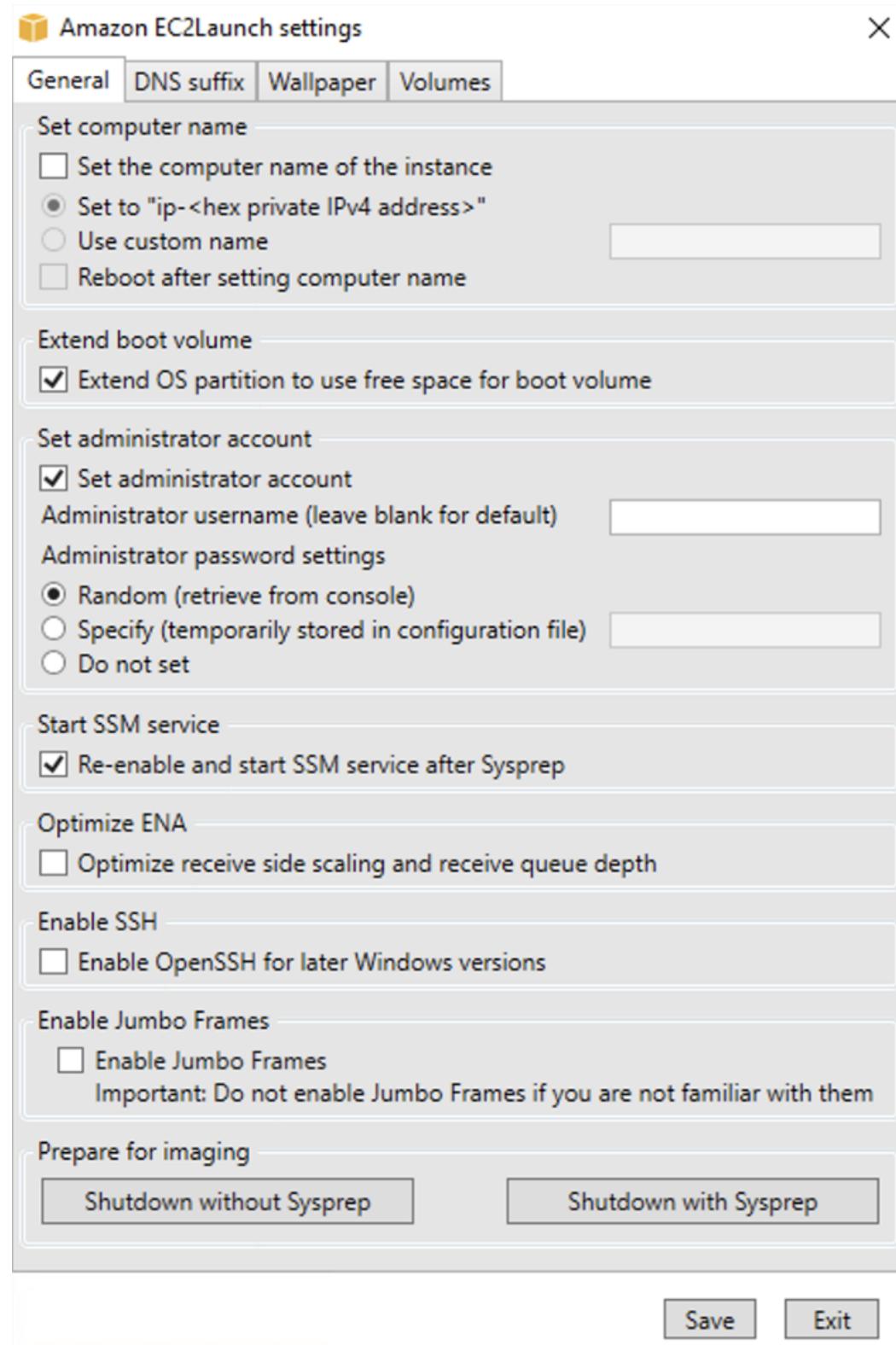
Os tópicos incluem:

- [Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2 \(p. 491\)](#)
- [Estrutura de diretório do EC2Launch v2 \(p. 497\)](#)
- [Configurar o EC2Launch v2 com a CLI \(p. 498\)](#)
- [Configuração de tarefas do EC2Launch v2 \(p. 503\)](#)
- [Códigos de saída e reinicializações do EC2Launch v2 \(p. 512\)](#)
- [EC2Launch v2 e Sysprep \(p. 512\)](#)

[Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2](#)

O procedimento a seguir descreve como usar a caixa de diálogo de configurações do EC2Launch v2 para habilitar ou desabilitar configurações.

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, escolha Todos os programas e navegue até as Configurações do EC2Launch.



3. Na guia Geral da caixa de diálogo Configurações do EC2Launch, você pode habilitar ou desabilitar as configurações a seguir.

- a. Definir o nome do computador

Se essa configuração estiver habilitada (por padrão, ela fica desabilitada), o nome do host atual será comparado com o nome de host desejado em cada inicialização. Se os nomes de host não corresponderem, o nome do host será redefinido e o sistema, opcionalmente, reinicializa para ficar com o novo nome de host. Se um nome de host personalizado não for especificado, ele será gerado usando o endereço IPv4 privado formatado hexadecimal, por exemplo, ip-AC1F4E6. Para impedir a modificação de um nome de host existente, não habilite essa configuração.

- b. Estender o volume de inicialização

Essa configuração amplia dinamicamente o Disk 0/Volume 0 para incluir qualquer espaço não particionado. Isso pode ser útil quando a instância for inicializada a partir de um volume do dispositivo raiz com tamanho personalizado.

- c. Definir a conta do administrador

Quando habilitado, você pode definir os atributos de nome de usuário e senha para a conta de administrador criada em sua máquina local. Se esse recurso não estiver habilitado, uma conta de administrador não será criada no sistema após o Sysprep. Forneça uma senha em adminPassword somente se adminPasswordtype for Specify.

Os tipos de senha são definidos da seguinte maneira:

- i. Random

O EC2Launch gera uma senha e criptografa-a usando a chave de usuário. O sistema desativa essa configuração depois da execução da instância, portanto, essa senha persistirá se a instância for reinicializada ou parada e iniciada.

- ii. Specify

O EC2Launch usa a senha especificada em adminPassword. Se a senha não atender aos requisitos de sistema, o EC2Launch gera uma senha aleatória. A senha é armazenada em agent-config.yml como texto não criptografado e será excluída depois que Sysprep definir a senha do administrador. O EC2Launch criptografa a senha usando a chave de usuário.

- iii. DoNothing

O EC2Launch usa a senha especificada no arquivo unattend.xml. Se você não especificar uma senha em unattend.xml, a conta de administrador será desativada.

- d. Iniciar o serviço SSM

Quando selecionado, o serviço Systems Manager é habilitado para começar após o Sysprep. O EC2Launch v2 executa todas as tarefas descritas [anteriormente \(p. 485\)](#) e o SSM Agent processa recursos do Systems Manager, como Run Command e State Manager.

Você pode usar Run Command para atualizar suas instâncias existentes e usar a versão mais recente do serviço do EC2Launch v2 e do SSM Agent. Para obter mais informações, consulte [Update SSM Agent by using Run Command \(Atualizar o SSM Agent usando o Run Command\)](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

- e. Otimizar ENA

Quando selecionadas, as configurações do ENA são definidas para garantir que as configurações Receive Side Scaling (Receber dimensionamento lateral) e Receive Queue Depth (Receber profundidade da fila) sejam otimizadas para a AWS. Para obter mais informações, consulte [Configurar afinidade de CPU RSS \(p. 1041\)](#).

f. Habilitar SSH

Essa configuração habilita o OpenSSH para versões posteriores do Windows a fim de permitir a administração remota do sistema.

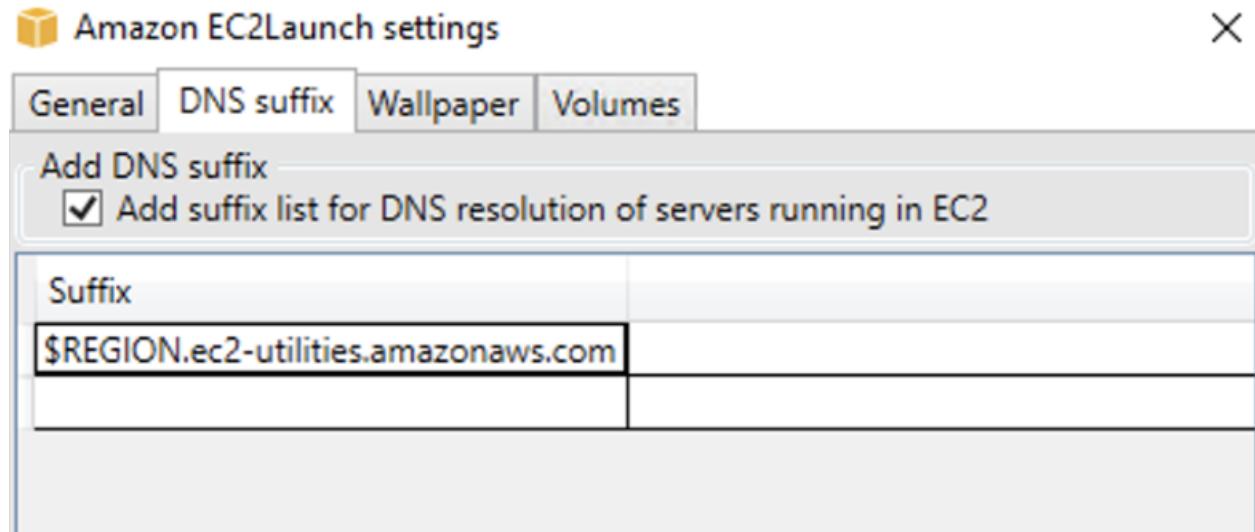
g. Ativar os frames jumbo

Selecione para ativar frames jumbo. Os frames jumbo podem ter efeitos não intencionais sobre suas comunicações de rede, portanto, certifique-se de entender como eles afetarão seu sistema antes de ativá-los. Para obter mais informações sobre os frames jumbo, consulte [Frames jumbo \(9.001 MTU\) \(p. 1057\)](#).

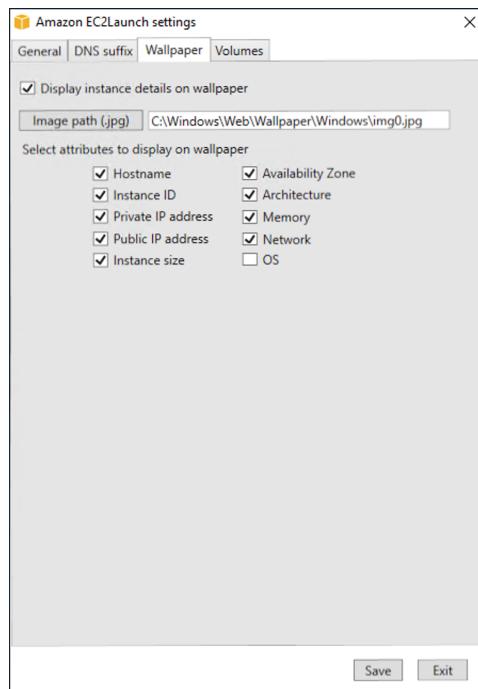
h. Preparar para imagens

Selecione se deseja que sua instância do EC2 seja desligada com ou sem Sysprep. Quando quiser executar o Sysprep com o EC2Launch v2, escolha Shutdown with Sysprep (Desligar com Sysprep).

4. Na guia Sufixo DNS, você pode selecionar se deseja adicionar uma lista de sufixos DNS para resolução DNS de servidores em execução no EC2, sem fornecer o nome de domínio totalmente qualificado. Os sufixos DNS podem conter as variáveis \$REGION e \$AZ. Somente sufixos que ainda não existem serão adicionados à lista.

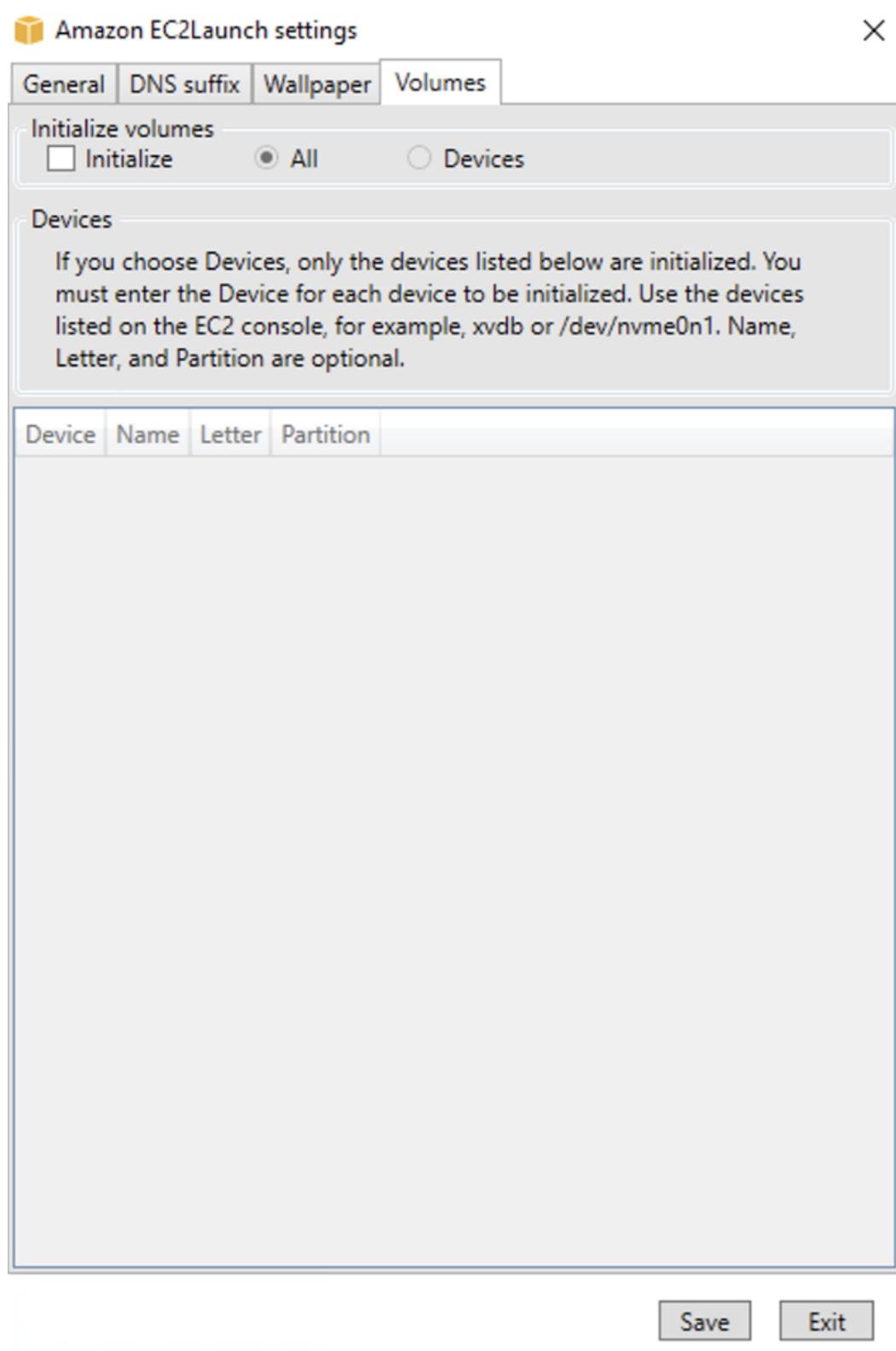


5. Na guia Papel de parede, você pode ativar a exibição de detalhes da instância selecionada no papel de parede. Você também tem a opção de escolher uma imagem personalizada. Os detalhes são gerados sempre que a sessão é iniciada. Desmarque a caixa de seleção para remover os detalhes da instância do papel de parede.



6. Na guia Volumes, selecione se deseja inicializar os volumes anexados à instância. A ativação define letras de unidade para quaisquer volumes adicionais e estende-as para usar o espaço disponível. Se você selecionar Todos, todos os volumes de armazenamento serão inicializados. Se você selecionar Dispositivos, somente os dispositivos especificados na lista serão inicializados. É preciso inserir cada dispositivo a ser inicializado. Use os dispositivos listados no console do EC2, por exemplo, xvdb ou /dev/nvme0n1. A lista suspensa exibe os volumes de armazenamento anexados à instância. Para inserir um dispositivo que não está anexado à instância, insira-o no campo de texto.

Nome, Letra e Partição são campos opcionais. Se nenhum valor for especificado para Partição, os volumes de armazenamento com mais de 2 TB serão inicializados com o tipo de partição GPT e os com menos de 2 TB serão inicializados com o tipo de partição MBR. Se os dispositivos estiverem configurados e um dispositivo não NTFS contiver uma tabela de partição ou os primeiros 4 KB do disco contiverem dados, o disco será ignorado e a ação será registrada.



Veja a seguir um exemplo de arquivo de configuração YAML criado a partir das configurações inseridas no diálogo EC2Launch.

```
version: 1.0
config:
  - stage: boot
    tasks:
      - task: extendRootPartition
  - stage: preReady
    tasks:
      - task: activateWindows
        inputs:
          activation:
            type: amazon
      - task: setDnsSuffix
        inputs:
          suffixes:
            - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
        - hostName
        - instanceId
        - privateIpAddress
        - publicIpAddress
        - instanceSize
        - availabilityZone
        - architecture
        - memory
        - network
  - stage: postReady
    tasks:
      - task: startSsm
```

Estrutura de diretório do EC2Launch v2

O EC2Launch v2 deve ser instalado nos seguintes diretórios:

- Binários de serviço: %ProgramFiles%\Amazon\EC2Launch
- Dados de serviço (configurações, arquivos de log e arquivos de estado): %ProgramData%\Amazon\EC2Launch

Note

Por padrão, o Windows oculta os arquivos e as pastas sob C:\ProgramData. Para visualizar os diretórios e arquivos do EC2Launch v2, digite o caminho no Windows Explorer ou altere as propriedades da pasta para os arquivos e as pastas ocultos.

O diretório %ProgramFiles%\Amazon\EC2Launch contém binários e bibliotecas compatíveis. Ele inclui os seguintes subdiretórios:

- **settings**
 - EC2LaunchSettingsUI.exe — interface de usuário para modificar o arquivo agent-config.yml
 - YamlDotNet.dll — DLL para oferecer suporte a algumas operações na interface do usuário
- **tools**

- `ebsnvme-id.exe` — ferramenta para examinar os metadados dos volumes do EBS na instância
- `AWSAcpISpcrReader.exe` — ferramenta para determinar a porta COM correta a ser usada
- `EC2LaunchEventMessage.dll` — DLL para oferecer suporte ao registro de eventos do Windows para o EC2Launch.
- `service`
 - `EC2LaunchService.exe` — Serviço do Windows executável que é iniciado quando o agente de inicialização é executado como um serviço.
- `EC2Launch.exe` — executável principal do EC2Launch
- `EC2LaunchAgentAttribution.txt` — atribuição para código usado dentro do EC2 Launch

O diretório `%ProgramData%\Amazon\EC2Launch` contém os seguintes subdiretórios. Todos os dados produzidos pelo serviço, incluindo logs, configuração e estado, são armazenados neste diretório.

- `config` — configuração

O arquivo de configuração do serviço é armazenado neste diretório como `agent-config.yml`. Esse arquivo pode ser atualizado de modo a modificar, adicionar ou remover tarefas padrão executadas pelo serviço. A permissão para criar arquivos neste diretório é restrita à conta de administrador para evitar o escalonamento de privilégios.

- `log` — logs de instância

Os logs do serviço (`agent.log`), o console (`console.log`), a performance (`bench.log`) e os erros (`error.log`) são armazenados neste diretório. Os arquivos de log são anexados a execuções subsequentes do serviço.

- `state` — dados de estado do serviço

O estado usado pelo serviço para determinar quais tarefas devem ser executadas é armazenado aqui. Há um arquivo `.run-once` que indica se o serviço já foi executado após Sysprep (portanto, as tarefas com frequência de uma vez serão ignoradas na próxima execução). Esse subdiretório inclui `state.json` e `previous-state.json` para rastrear o status de cada tarefa.

- `sysprep` — Sysprep

Esse diretório contém arquivos usados para determinar quais operações executar pelo Sysprep ao criar uma AMI do Windows personalizada que pode ser reutilizada.

Configurar o EC2Launch v2 com a CLI

Você pode usar a Interface de Linhas de Comando (CLI) para definir suas configurações do EC2Launch e gerenciar o serviço. A seção a seguir contém descrições e informações de uso dos comandos da CLI que podem ser usados para gerenciamento do EC2Launch v2.

Comandos

- [collect-logs \(p. 499\)](#)
- [get-agent-config \(p. 499\)](#)
- [list-volumes \(p. 500\)](#)
- [reset \(p. 500\)](#)
- [run \(p. 500\)](#)
- [status \(p. 501\)](#)
- [sysprep \(p. 501\)](#)
- [validate \(p. 502\)](#)
- [version \(p. 502\)](#)

- [wallpaper \(p. 503\)](#)

collect-logs

Coleta arquivos de log para o EC2Launch, compacta os arquivos e os coloca em um diretório especificado.

Exemplo

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Uso

`ec2launch collect-logs [flags]`

Sinalizadores

`-h, --help`

ajuda para `collect-logs`

`-o, --output string`

caminho para arquivos de log de saída compactados

get-agent-config

Imprime `agent-config.yml` no formato especificado (JSON ou YAML). Se nenhum formato for especificado, `agent-config.yml` será impresso no formato especificado anteriormente.

Exemplo

```
ec2launch get-agent-config -f json
```

Exemplo 2

Os seguintes comandos do PowerShell mostram como editar e salvar o arquivo `agent-config` no formato JSON.

```
$config = ec2launch get-agent-config --format json | ConvertFrom-Json
$jumboFrame =@"
{
    "task": "enableJumboFrames"
}
@"
$config.config | %{{if($_.stage -eq 'postReady'){$_.tasks += (ConvertFrom-Json -InputObject
    $jumboFrame)}}}
$config | ConvertTo-Json -Depth 6 | Out-File -encoding UTF8 $env:ProgramData/Amazon/
EC2Launch/config/agent-config.yml
```

Uso

`ec2launch get-agent-config [flags]`

Sinalizadores

`-h, --help`

ajuda para get-agent-config

-f, --format string

formato de saída do arquivo agent-config: json, yaml

[list-volumes](#)

Lista todos os volumes de armazenamento anexados à instância, incluindo volumes temporários e do EBS.

Exemplo

```
ec2launch list-volumes
```

Uso

`ec2launch list-volumes`

Sinalizadores

-h, --help

ajuda para `list-volumes`

[reset](#)

Exclui o arquivo `.runonce` para que as tarefas especificadas a serem executadas uma vez sejam realizadas na próxima execução; também exclui os logs de serviço e sysprep.

Exemplo

```
ec2launch reset -c
```

Uso

`ec2launch reset [flags]`

Sinalizadores

-b, --block

bloqueia o comando `reset` até que o serviço pare. Se o comando de reiniciar for executado com o comando `--block` como parte da tarefa `executeScript`, o argumento `detach` deve ser definido como verdadeiro. Para obter mais informações, consulte o Exemplo 4 em [executeScript \(p. 505\)](#).

-c, --clean

limpa os logs da instância antes de `reset`

-h, --help

ajuda para `reset`

[run](#)

Executa o EC2Launch v2.

Exemplo

```
ec2launch run
```

Uso

```
ec2launch run [flags]
```

Sinalizadores

```
-h, --help
```

ajuda para run

status

Obtém o status do serviço de EC2Launch. Opcionalmente, bloqueia o processo até que o serviço seja concluído. O código de saída do processo determina o estado do serviço:

- 0 — o serviço foi executado e foi bem-sucedido.
- 1 — o serviço foi executado e apresentou falha.
- 2 — o serviço ainda está em execução.
- 3: o serviço está em um estado desconhecido. O estado do serviço não está em execução ou está parado.
- 4: ocorreu um erro ao tentar retornar o estado do serviço.
- 5: o serviço não está em execução e o status da última execução conhecida é desconhecido. Isso pode significar uma das seguintes opções:
 - tanto o state.json quanto o previous-state.json foram excluídos.
 - o previous-state.json está corrompido.

Este é o estado do serviço depois de executar o comando [reset \(p. 500\)](#).

Exemplo:

```
ec2launch status -b
```

Uso

```
ec2launch status [flags]
```

Sinalizadores

```
-b,--block
```

bloqueia o processo até que os serviços concluam a execução

```
-h,--help
```

ajuda para status

sysprep

Redefine o estado do serviço, atualiza unattend.xml, desativa o RDP e executa Sysprep.

Exemplo:

```
ec2launch sysprep
```

Uso

```
ec2launch sysprep [flags]
```

Sinalizadores

-b,--block

bloqueia o comando `sysprep` até que o serviço pare. Se o comando de reiniciar for executado com o comando `--block` como parte da tarefa `executeScript`, o argumento `detach` deve ser definido como verdadeiro. Para obter mais informações, Consulte o Exemplo 4 em [executeScript \(p. 505\)](#).

-c,--clean

limpa os logs da instância antes de `sysprep`

-h,--help

ajuda para `Sysprep`

-s,--shutdown

desliga a instância após `sysprep`

validate

Valida o arquivo `agent-config` C:\ProgramData\Amazon\EC2LaunchAgent\config\agent-config.yml.

Exemplo

```
ec2launch validate
```

Uso

```
ec2launch validate [flags]
```

Sinalizadores

-h , --help

ajuda para `validate`

version

Obtém a versão executável.

Exemplo

```
ec2launch version
```

Uso

```
ec2launch version [flags]
```

Sinalizadores

-h, --help

ajuda para version

wallpaper

Define o novo papel de parede para o caminho de papel de parede fornecido (arquivo .jpg) e exibe os detalhes da instância selecionada.

Exemplo

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,instanceSize,availabilityZone,architect
```

Uso

`ec2launch wallpaper [flags]`

Sinalizadores

`--attributes strings`

wallpaperAtributos do

`-h, --help`

ajuda para wallpaper

`-p, --path string`

wallpaperCaminho do arquivo

Configuração de tarefas do EC2Launch v2

Esta seção inclui as tarefas, detalhes e exemplos de configuração para os arquivos `agent-config.yml` e `user-data.yml`.

Tarefas e exemplos

- [activateWindows \(p. 504\)](#)
- [enableJumboFrames \(p. 504\)](#)
- [enableOpenSsh \(p. 504\)](#)
- [executeProgram \(p. 505\)](#)
- [executeScript \(p. 505\)](#)
- [extendRootPartition \(p. 507\)](#)
- [initializeVolume \(p. 507\)](#)
- [optimizeEna \(p. 508\)](#)
- [setAdminAccount \(p. 508\)](#)
- [setDnsSuffix \(p. 509\)](#)
- [setHostName \(p. 509\)](#)
- [setWallpaper \(p. 509\)](#)
- [startSsm \(p. 510\)](#)
- [sysprep \(p. 510\)](#)
- [writeFile \(p. 511\)](#)

- [Exemplo: agent-config.yml \(p. 511\)](#)
- [Exemplo: dados do usuário \(p. 512\)](#)

activateWindows

Ativa o Windows em relação a um conjunto de servidores de AWS KMS.

Frequência — uma vez

AllowedStages — [PreReady]

Entradas —

activation: (mapa)

type: (string) tipo de ativação a usar, defina como amazon

Exemplo

```
task: activateWindows
inputs:
  activation:
    type: amazon
```

enableJumboFrames

Habilita frames jumbo, que aumentam a MTU (unidade de transmissão máxima) do adaptador de rede. Para obter mais informações, consulte [Frames jumbo \(9.001 MTU\) \(p. 1057\)](#).

Frequência — sempre

AllowedStages — [PostReady, UserData]

Entradas — nenhuma

Exemplo

```
task: enableJumboFrames
```

Habilita o Windows OpenSSH e adiciona a chave pública da instância à pasta de chaves autorizadas.

Frequência — uma vez

AllowedStages — [PreReady, UserData]

Entradas — nenhuma

Exemplo

O exemplo a seguir mostra como habilitar o OpenSSH em uma instância e adicionar a chave pública da instância à pasta de chaves autorizadas. Essa configuração funciona somente em instâncias que executam o Windows Server 2019 e versões posteriores.

```
task: enableOpenSsh
```

executeProgram

Executa um programa com argumentos opcionais e uma frequência especificada.

Frequência — exibir Entradas

AllowedStages — [PostReady, UserData]

Entradas —

frequency: (string) once ou always

path: (string) caminho para o executável

arguments: (lista de strings) lista de argumentos de string a serem transmitidos para o executável

runAs: (string) deve ser definido como localSystem

Exemplo

O exemplo a seguir mostra como executar um arquivo executável que já está em uma instância.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\Users\Administrator\Desktop\setup.exe
  arguments: ['-quiet']
```

Exemplo 2

O exemplo a seguir mostra como executar um arquivo executável que já está em uma instância. Essa configuração instala um arquivo VLC .exe presente na unidade C: da instância. /L=1033 e /S são argumentos de VLC passados como uma lista de strings com o arquivo VLC .exe.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\vlc-3.0.11-win64.exe
  arguments: ['/L=1033','/S']
  runAs: localSystem
```

executeScript

Executa um script com argumentos opcionais e uma frequência especificada.

Frequência — exibir Entradas

AllowedStages — [PostReady, UserData]

Entradas —

detach: (booleano) indica se o script é executado como um processo desvinculado. Quando ativado, o EC2Launch v2 executa o script simultaneamente com outras tarefas e não lida com códigos de saída, como 3010, para reiniciar a instância.

frequency: (string) once ou always

type: (string) batch ou powershell

arguments: (lista de strings) lista de argumentos de string a serem transmitidos ao shell. Esse parâmetro não é compatível com type é definido como batch.

content: (string) conteúdo do script

runAs: (string) admin ou localSystem

detach: (booleano) é o padrão para false. Defina como true, se o script deve ser executado no modo desvinculado, em que o EC2Launch o executa e continua com outras tarefas. Os códigos de saída de script não têm efeito nesse modo.

Exemplo

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  content: |
    Get-Process | Out-File -FilePath .\Process.txt
runAs: localSystem
```

Exemplo 2

O exemplo a seguir mostra como executar um script do PowerShell em uma instância do EC2. Essa configuração cria um arquivo de texto na unidade C:.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: admin
  content: |
    New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
    Set-Content 'C:\PowerShellTest.txt' "hello world"
```

Exemplo 3

O exemplo a seguir mostra um script idempotente que reinicializa uma instância várias vezes.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: localSystem
  content: |
    $name = $env:ComputerName
    if ($name -ne $desiredName) {
      Rename-Computer -NewName $desiredName
      exit 3010
    }
    $domain = Get-ADDomain
    if ($domain -ne $desiredDomain)
    {
      Add-Computer -DomainName $desiredDomain
      exit 3010
    }
    $telnet = Get-WindowsFeature -Name Telnet-Client
    if (-not $telnet.Installed)
    {
      Install-WindowsFeature -Name "Telnet-Client"
      exit 3010
    }
```

}

Exemplo 4

Você pode executar comandos da CLI do EC2Launch v2 como parte de scripts. `reset` e `sysprep` devem incluir o comando `--block`, pois dependem de o agente encerrar primeiro. Quando o `--block` é usado, o argumento `detach` para a tarefa deve ser definido como verdadeiro. Um impasse acontece quando você usa o sinalizador `--block` em um script não desvinculado. Os comandos detectam o impasse potencial e saem com um erro. O exemplo a seguir mostra um script que reinicia o estado do agente após a conclusão da execução do agente.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: localSystem
  detach: true
  content: |-
    & 'C:\Program Files\Amazon\EC2Launch\ec2launch.exe' reset -c -b
```

extendRootPartition

Estende o volume raiz para usar todo o espaço disponível no disco.

Frequência — uma vez

AllowedStages — [Boot]

Entradas — nenhuma

Exemplo

```
task: extendRootPartition
```

initializeVolume

Inicializa volumes anexados à instância para que eles sejam ativados e particionados. Quaisquer volumes detectados como não vazios não são inicializados. Um volume é considerado vazio se seus primeiros 4 KiB estiverem vazios ou se o volume não tiver um [layout de unidade reconhecível pelo Windows](#). O campo de volume `letter` é sempre aplicado quando essa tarefa é executada, independentemente se a unidade já foi inicializada ou não.

Frequência — sempre

AllowedStages — [PostReady, UserData]

Entradas —

`initialize`: (string) tipo de estratégia de inicialização a usar; all ou devices

`devices`: (lista de mapas)

`device`: identificador de dispositivo usado ao criar a instância; alguns exemplos são xvdb, xvdf ou /dev/nvme0n1

`name`: (string) nome da unidade a atribuir

`letter`: (string) letra de unidade a atribuir

`partition`: (string) tipo de particionamento a usar; mbr ou gpt

Exemplo 1

O exemplo a seguir mostra entradas para a tarefa `InitializeVolume` para definir os volumes selecionados a serem inicializados.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
    - device: xvdb
      name: MyVolumeOne
      letter: D
      partition: mbr
    - device: /dev/nvme0n1
      name: MyVolumeTwo
      letter: E
      partition: gpt
```

Exemplo 2

O exemplo a seguir mostra como inicializar volumes do EBS que estão anexados a uma instância. Essa configuração inicializará todos os volumes vazios do EBS que estão conectados à instância. Se um volume não estiver vazio, ele não será inicializado.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Otimiza as configurações do ENA com base no tipo de instância atual; pode reinicializar a instância.

Frequência — sempre

AllowedStages — [`PostReady`, `UserData`]

Entradas — nenhuma

Exemplo

```
task: optimizeEna
```

setAdminAccount

Define atributos para a conta de administrador padrão criada na máquina local.

Frequência — uma vez

AllowedStages — [`PreReady`]

Entradas —

`name`: (string) nome da conta de administrador

`password`: (mapa)

`type`: (string) estratégia para definir a senha como `static`, `random` ou `doNothing`

`data`: (string) armazena dados se o campo `type` for estático

Exemplo

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
    type: random
```

setDnsSuffix

Adiciona sufixos DNS à lista de sufixos de pesquisa. Somente sufixos que ainda não existem são adicionados à lista.

Frequência — sempre

AllowedStages — [PreReady]

Entradas —

suffixes: (lista de strings) lista de um ou mais sufixos DNS válidos; variáveis de substituição válidas são \$REGION e \$AZ

Exemplo

```
task: setDnsSuffix
inputs:
  suffixes:
    - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Define o nome do host do computador como uma string personalizada ou, se o hostName não for especificado, o endereço IPv4 privado.

Frequência — sempre

AllowedStages — [PostReady, UserData]

Entradas —

hostName: (string) nome do host opcional, que deve ser formatado conforme o seguinte.

- Ele deve ter 15 caracteres ou menos
- Ele deve conter apenas caracteres alfanuméricos (a-z, A-Z, 0-9) e hífen (-).
- Ele não deve consistir inteiramente em caracteres numéricos.

reboot: (booliano) indica se uma reinicialização é permitida quando o nome de host é alterado

Exemplo

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Configura a instância com papel de parede personalizado que exibe atributos de instância.

Frequência — sempre

AllowedStages — [PreReady, UserData]

Entradas —

path: (string) caminho para um arquivo .jpg local para uso como imagem de papel de parede

attributes: (lista de strings) lista de atributos para adicionar ao papel de parede; hostName, instanceId, privateIpAddress, publicIpAddress, instanceSize, availabilityZone, architecture, memory ou network

Exemplo

```
task: setWallpaper
inputs:
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
    - hostName
    - instanceId
    - privateIpAddress
    - publicIpAddress
```

startSsm

Iniciar o serviço Systems Manager (SSM) após o Sysprep.

Frequência — sempre

AllowedStages — [PostReady, UserData]

Entradas — nenhuma

Exemplo

```
task: startSsm
```

sysprep

Redefine o estado do serviço, atualiza unattend.xml, desativa o RDP e executa Sysprep. Esta tarefa só é executada depois que todas as outras tarefas forem concluídas

Frequência — uma vez

AllowedStages — [UserData]

Entradas —

clean: (booliano) limpa os logs de instância antes de executar o Sysprep

shutdown: (booliano) desliga a instância depois de executar o Sysprep

Exemplo

```
task: sysprep
inputs:
  clean: true
  shutdown: true
```

writeFile

Grava um arquivo em um destino.

Frequência — exibir Entradas

AllowedStages — [PostReady, UserData]

Entradas —

frequency: (string) once ou always

destination: (string) caminho no qual gravar o conteúdo

content: (string) texto a gravar no destino

Exemplo

```
task: writeFile
inputs:
- frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Exemplo: agent-config.yml

O exemplo a seguir mostra as configurações do arquivo de configuração agent-config.yml.

```
version: 1.0
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
      - memory
      - network
- stage: postReady
  tasks:
  - task: startSsm
```

Exemplo: dados do usuário

Para obter mais informações sobre as funções de usuário, consulte [Executar comandos na instância do Windows na inicialização \(p. 614\)](#).

O exemplo a seguir mostra as configurações para dados do usuário.

```
version: 1.0
tasks:
- task: executeScript
  inputs:
    - frequency: always
      type: powershell
      runAs: localSystem
      content: |
        New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

O seguinte formato é compatível com a versão anterior desse serviço. Ele é executado como uma tarefa `executeScript` no estágio `UserData`. Para imitar o comportamento da versão anterior, ele será configurado para ser executado como um processo desvinculado.

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Códigos de saída e reinicializações do EC2Launch v2

Você pode usar EC2Launch v2 para definir como os códigos de saída são manipulados por seus scripts. Por padrão, o código de saída do último comando executado em um script é relatado como o código de saída de todo o script. Por exemplo, se um script incluir três comandos e o primeiro comando falhar, mas os seguintes forem bem-sucedidos, o status de execução será relatado como `success` porque o comando final foi bem-sucedido.

Se você quiser que um script reinicialize uma instância, deverá especificar `exit 3010` no seu script, mesmo quando a reinicialização for a última etapa do script. `exit 3010` instrui EC2Launch v2 a reiniciar a instância e chamar o script novamente até que ele retorne um código de saída que não seja 3010 ou até que a contagem máxima de reinicialização seja alcançada. O EC2Launch v2 permite um máximo de 5 reinicializações por tarefa. Se você tentar reiniciar uma instância a partir de um script usando um mecanismo diferente, como `Restart-Computer`, o status de execução do script será inconsistente. Por exemplo, ele pode ficar preso em um loop de reinicialização ou não executar a reinicialização.

Se você estiver usando um formato de dados de usuário herdado compatível com agentes mais antigos, os dados do usuário poderão ser executados mais vezes do que você pretende. Para obter mais informações, consulte [O serviço executa dados do usuário mais de uma vez \(p. 514\)](#) na seção Solução de problemas.

EC2Launch v2 e Sysprep

O serviço EC2Launch v2 executa o Sysprep, uma ferramenta da Microsoft que permite a criação de uma AMI personalizada do Windows que pode ser reutilizada. Quando o EC2Launch v2 acessa o Sysprep, ela usa os arquivos em `%ProgramData%\Amazon\EC2Launch` para determinar quais operações devem ser executadas. Você pode editar esses arquivos indiretamente usando a caixa de diálogo Configurações do EC2Launch ou diretamente usando um editor de YAML ou um editor de texto. Contudo, há algumas configurações avançadas que não estão disponíveis na caixa de diálogo Configurações do EC2Launch, portanto, você deve editar as entradas diretamente.

Se você criar AMIs com base em uma instância depois de atualizar suas configurações, as configurações novas serão aplicadas a qualquer instância executada pela nova AMI. Para obter informações sobre como criar uma AMI, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#).

Solucionar problemas do EC2Launch v2

Esta seção mostra cenários comuns de solução de problemas para o EC2Launch v2, informações sobre como exibir logs de eventos do Windows e saída e mensagens do log do console.

Tópicos de solução de problemas

- [Cenários comuns de solução de problemas \(p. 513\)](#)
- [Logs de eventos do Windows \(p. 515\)](#)
- [Saída do log do console do EC2Launch v2 \(p. 518\)](#)

Cenários comuns de solução de problemas

Esta seção mostra cenários comuns de solução de problemas e etapas para resolução.

Cenários

- [Falha no serviço ao definir o papel de parede \(p. 513\)](#)
- [Falha no serviço ao executar dados do usuário \(p. 513\)](#)
- [O serviço executa uma tarefa apenas uma vez \(p. 513\)](#)
- [Falha no serviço ao executar uma tarefa \(p. 514\)](#)
- [O serviço executa dados do usuário mais de uma vez \(p. 514\)](#)
- [As tarefas agendadas do EC2Launch v1 não conseguem ser executadas após a migração para o EC2Launch v2 \(p. 514\)](#)
- [Falha no serviço ao executar uma tarefa \(p. 514\)](#)
- [O serviço inicializa um volume do EBS que não está vazio \(p. 515\)](#)

Falha no serviço ao definir o papel de parede

Resolution

1. Verifique se %AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\setwallpaper.lnk existe.
2. Verifique %ProgramData%\Amazon\EC2Launch\log\agent.log para saber se ocorreram erros.

Falha no serviço ao executar dados do usuário

Causa possível: a falha no serviço pode ter ocorrido antes da execução dos dados do usuário.

Resolution

1. Verifique %ProgramData%\Amazon\EC2Launch\state\previous-state.json.
2. Veja se boot, network, preReady e postReadyLocalData foram todos marcados como sucesso.
3. Se um dos estágios falhar, verifique se há erros específicos %ProgramData%\Amazon\EC2Launch\log\agent.log.

O serviço executa uma tarefa apenas uma vez

Resolution

1. Verifique a frequência da tarefa.
2. Se o serviço já tiver sido executado após Sysprep e a frequência da tarefa estiver definida como once, a tarefa não será executada novamente.

3. Defina a frequência da tarefa como `always` se você quiser que ela execute a tarefa sempre que o EC2Launch v2 for executado.

Falha no serviço ao executar uma tarefa

Resolution

1. Verifique as entradas mais recentes em `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Se não ocorrerem erros, tente executar o serviço manualmente a partir de `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe"` run para ver se as tarefas foram bem-sucedidas.

O serviço executa dados do usuário mais de uma vez

Resolution

Os dados do usuário são tratados de forma diferente entre o EC2Launch v1 e o EC2Launch v2. O EC2Launch v1 executa dados do usuário como uma tarefa programada na instância quando `persist` é definido como `true`. Se `persist` estiver definido como `false`, a tarefa não será programada mesmo quando ela sair com uma reinicialização ou for interrompida durante a execução.

EC2Launch v2 executa dados do usuário como uma tarefa de agente e rastreia seu estado de execução. Se os dados do usuário emitirem uma reinicialização do computador ou se os dados do usuário tiverem sido interrompidos durante a execução, o estado de execução persistirá `pending` e os dados do usuário serão executados novamente na próxima inicialização da instância. Se você quiser impedir que o script de dados do usuário seja executado mais de uma vez, torne o script idempotente.

O exemplo a seguir de script idempotente define o nome do computador e se junta a um domínio.

```
<powershell>
    $name = $env:computername
    if ($name -ne $desiredName) {
        Rename-Computer -NewName $desiredName
    }
    $domain = Get-ADDomain
    if ($domain -ne $desiredDomain)
    {
        Add-Computer -DomainName $desiredDomain
    }
    $telnet = Get-WindowsFeature -Name Telnet-Client
    if (-not $telnet.Installed)
    {
        Install-WindowsFeature -Name "Telnet-Client"
    }
</powershell>
<persist>false</persist>
```

As tarefas agendadas do EC2Launch v1 não conseguem ser executadas após a migração para o EC2Launch v2

Resolution

A ferramenta de migração não detecta qualquer tarefa agendada vinculada aos scripts do EC2Launch v1; portanto, ela não configura automaticamente essas tarefas no EC2Launch v2. Para configurar essas tarefas, edite o arquivo [agent-config.yml \(p. 503\)](#) ou use a [caixa de diálogo de configurações do EC2Launch v2 \(p. 491\)](#). Por exemplo, se uma instância tiver uma tarefa agendada que executa `InitializeDisks.ps1`, depois de executar a ferramenta de migração, você deverá especificar os volumes que deseja inicializar na caixa de diálogo de configurações do EC2Launch v2. Consulte a Etapa

6 do procedimento para [Alterar configurações usando a caixa de diálogo de configurações do EC2Launch v2 \(p. 491\)](#).

Falha no serviço ao executar uma tarefa

Resolution

1. Verifique as entradas mais recentes em %ProgramData%\Amazon\EC2Launch\log\agent.log.
2. Se não ocorrerem erros, tente executar o serviço manualmente a partir de "%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run para ver se as tarefas foram bem-sucedidas.

O serviço inicializa um volume do EBS que não está vazio

Resolution

Antes de inicializar um volume, o EC2Launch v2 tenta detectar se ele está vazio. Se um volume não estiver vazio, ele ignorará a inicialização. Quaisquer volumes detectados como não vazios não são inicializados. Um volume é considerado vazio se seus primeiros 4 KiB estiverem vazios ou se o volume não tiver um [layout de unidade reconhecível pelo Windows](#). Um volume que foi inicializado e formatado em um sistema Linux não tem um layout de unidade reconhecível pelo Windows, por exemplo MBR ou GPT. Portanto, ele será considerado vazio e será inicializado. Se você quiser preservar esses dados, não confie na detecção de unidade vazia do EC2Launch v2. Em vez disso, especifique os volumes que você gostaria de inicializar na [caixa de diálogo de configurações do EC2Launch v2 \(p. 491\)](#) (consulte a etapa 6) ou no [agent-config.yml \(p. 507\)](#).

Logs de eventos do Windows

O EC2Launch v2 publica logs de eventos do Windows para eventos importantes, como a inicialização do serviço, o Windows pronto, e o sucesso e a falha da tarefa. Identificadores de eventos identificam exclusivamente um evento específico. Cada evento contém informações de estágio, tarefa e nível e uma descrição. É possível definir gatilhos para eventos específicos usando o identificador de eventos.

Os IDs de evento fornecem informações sobre um evento e identificam alguns eventos de forma exclusiva. O dígito menos significativo de um ID de evento indica a gravidade de um evento.

Evento	Dígito menos significativo
Success	. . . 0
Informational	. . . 1
Warning	. . . 2
Error	. . . 3

Os eventos relacionados ao serviço, gerados quando o serviço é iniciado ou interrompido, incluem um identificador de evento de um dígito.

Evento	Identificador de um dígito
Success	0
Informational	1
Warning	2
Error	3

As mensagens de evento para eventos do `EC2LaunchService.exe` começam com `Service::`. As mensagens de evento para eventos do `EC2Launch.exe` não começam com `Service::`.

Os IDs de evento de quatro dígitos incluem informações sobre o estado, a tarefa e a gravidade de um evento.

Tópicos

- [Formato de ID do evento \(p. 516\)](#)
- [Exemplos de ID de evento \(p. 516\)](#)
- [Esquema de log de eventos do Windows \(p. 517\)](#)

[Formato de ID do evento](#)

A tabela a seguir mostra o formato de um identificador de eventos do EC2Launch v2.

3	2 1	0
S	T	L

As letras e números na tabela representam o tipo de evento e as definições a seguir.

Tipo de evento	Definição
S (Estágio)	0 - Mensagem de nível de serviço 1 - Inicialização 2 - Rede 3 - PreReady 5 - O Windows está pronto 6 - PostReady 7 - Dados do usuário
T (Tarefa)	As tarefas representadas pelos dois valores correspondentes são diferentes para cada estágio. Para visualizar a lista completa de eventos, consulte Esquema de log de eventos do Windows (p. 517) .
L (Nível do evento)	0 - Êxito 1 - Informativo 2 - Aviso 3 - Erro

[Exemplos de ID de evento](#)

Veja a seguir alguns exemplos de IDs de evento.

- 5000 - o Windows está pronto para ser usado
- 3010 - êxito ao ativar a tarefa do Windows no estágio PreReady
- 6013 - A tarefa Definir papel de parede no estágio PostReady Local Data encontrou um erro

Esquema de log de eventos do Windows

Messageld/ID do evento	Mensagem do evento
. . . 0	Success
. . . 1	Informational
. . . 2	Warning
. . . 3	Error
x	EC2Launch service-level logs
0	EC2Launch service exited successfully
1	EC2Launch service informational logs
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix

Messageld/ID do evento	Mensagem do evento
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

Saída do log do console do EC2Launch v2

Esta seção contém uma saída de log do console de exemplo para EC2Launch v2 e lista todas as mensagens de erro de log do console do EC2Launch v2 para ajudar você a solucionar problemas.

Outputs

- [Saída do log do console do EC2Launch v2 \(p. 518\)](#)
- [Mensagens de log do console do EC2Launch v2 \(p. 519\)](#)

Saída do log do console do EC2Launch v2

Veja a seguir um exemplo de saída de log do console para EC2Launch v2.

```
2020/08/13 17:25:12Z: Windows is being configured. SysprepState=IMAGE_STATE_UNDEPLOYABLE
```

```
2020/08/13 17:27:44Z: Windows is being configured. SysprepState=IMAGE_STATE_UNDEPLOYABLE
2020/08/13 17:28:02Z: Windows sysprep configuration complete.
2020/08/13 17:28:03Z: Message: Waiting for meta-data accessibility...
2020/08/13 17:28:03Z: Message: Meta-data is now available.
2020/08/13 17:28:03Z: AMI Origin Version: 2020.07.15
2020/08/13 17:28:03Z: AMI Origin Name: EC2LaunchV2_Preview-Windows_Server-2012_R2_RTM-
English-Full-Base
2020/08/13 17:28:03Z: OS: Microsoft Windows NT 6.3.9600
2020/08/13 17:28:03Z: OsVersion: 6.3
2020/08/13 17:28:03Z: OsProductName: Windows Server 2012 R2 Standard
2020/08/13 17:28:03Z: OsBuildLabEx: 9600.19761.amd64fre.winblue_ltsb.200610-0600
2020/08/13 17:28:03Z: OsCurrentBuild: 9600
2020/08/13 17:28:03Z: Language: en-US
2020/08/13 17:28:03Z: TimeZone: GMT
2020/08/13 17:28:03Z: Offset: UTC +0000
2020/08/13 17:28:03Z: Launch: EC2 Launch v2.0.0
2020/08/13 17:28:03Z: AMI-ID: ami-1a2b3c4d
2020/08/13 17:28:03Z: Instance-ID: i-1234567890abcdef0
2020/08/13 17:28:03Z: Instance Type: t2.nano
2020/08/13 17:28:07Z: Driver: AWS PV Driver Package v8.3.3
2020/08/13 17:28:07Z: RDPCERTIFICATE-SUBJECTNAME: EC2AMAZ-A1B2C3D
2020/08/13 17:28:07Z: RDPCERTIFICATE-THUMBPRINT: A1B2C3D4E5
2020/08/13 17:28:12Z: SSM: Amazon SSM Agent v2.3.842.0
2020/08/13 17:28:13Z: Username: Administrator
2020/08/13 17:28:13Z: Password: <Password>
A1B2C3D4E5F6G7H8I9J10K11L12M13N14O15P16Q17
</Password>
2020/08/13 17:28:13Z: Message: Windows is Ready to use
```

Mensagens de log do console do EC2Launch v2

Veja a seguir uma lista de todas as mensagens de log do console do EC2Launch v2.

```
Message: Error EC2Launch service is stopping. {error message}
Error setting up EC2Launch agent folders
See instance logs for detail
Error stopping service
Error initializing service
Message: Windows sysprep configuration complete
Message: Invalid administrator username: {invalid username}
Message: Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
```

```
Microsoft-Hyper-V is installed.  
Unable to get service status for vmms  
Microsoft-Hyper-V is {status}  
SSM: Amazon SSM Agent {version}  
AWS VSS Version: {version}  
Message: Windows sysprep configuration complete  
Message: Windows is being configured. SysprepState is {state}  
Windows is still being configured. SysprepState is {state}  
Message: Windows is Ready to use  
Message: Waiting for meta-data accessibility...  
Message: Meta-data is now available.  
Message: Still waiting for meta-data accessibility...  
Message: Failed to find primary network interface...retrying...
```

Históricos de versões do EC2Launch v2

Históricos de versões

- [Histórico de versões do EC2Launch v2 \(p. 520\)](#)
- [Histórico de versões da ferramenta de migração do EC2Launch v2 \(p. 521\)](#)

Histórico de versões do EC2Launch v2

A tabela a seguir descreve as versões liberadas do EC2Launch v2.

Versão	Detalhes	Data de lançamento
2.0.592	<ul style="list-style-type: none">Corrigiu o bug para relatar corretamente o status do estágio.Remove alarmes falsos de mensagens de erro quando os arquivos de log são fechados.Adicionou telemetria.	31 de agosto de 2021
2.0.548	<ul style="list-style-type: none">Adicionou zeros à esquerda para nome de host IP hexadecimal.Corrigiu permissões de arquivo para a tarefa enableOpenSsh.Corrigiu a falha no comando sysprep.	4 de agosto de 2021
2.0.470	<ul style="list-style-type: none">Corrigiu o erro na etapa de rede para esperar que o DHCP atribua um IP à instância.Correções de erros com setDnsSuffix quando a chave de registro SearchList não existe.Corrigiu o bug na lógica de devolução de DNS em setDnsSuffix.Adicionou roteamentos de rede após reinicializações intermediárias.Permite que initializeVolume volte a escrever volumes existentes.Remove informações adicionais do subcomando da versão.	20 de julho de 2021
2.0.285	<ul style="list-style-type: none">Adicionou opção de executar scripts de usuário em um processo desanexado.Os dados de usuário legados agora são executados em um processo desanexado, que é um comportamento semelhante ao agente de inicialização anterior.Adicionou o sinalizador CLI ao sysprep e aos comandos reset, o que os permite bloquear até que o serviço pare.Restringe as permissões da pasta de configuração.	8 de março de 2021

Versão	Detalhes	Data de lançamento
2.0.207	<ul style="list-style-type: none"> Adiciona o campo <code>hostName</code> opcional à tarefa <code>setHostName</code>. Corrigi bugs de reinicialização. As tarefas de reinicialização <code>executeScript</code> e <code>executeProgram</code> serão marcadas como em execução. Adiciona mais códigos de retorno ao comando de status. Adiciona o serviço de bootstrap para corrigir problema de startup ao executar no tipo de instância <code>t2.nano</code>. Corrigi o modo de instalação limpa para remover arquivos não rastreados pelo instalador. 	2 de fevereiro de 2021
2.0.160	<ul style="list-style-type: none"> Corrigi o comando <code>validate</code> para detectar nomes de estágios inválidos. Adiciona o comando <code>w32tm resync</code> na tarefa <code>addroutes</code>. Corrigi o problema com a alteração da ordem de pesquisa de sufixos DNS. Adiciona condições de verificação para relatar melhor dados inválidos do usuário. 	4 de dezembro de 2020
2.0.153	Adiciona a funcionalidade Sysprep em <code>UserData</code> .	3 de novembro de 2020
2.0.146	<ul style="list-style-type: none"> Corrigi o problema com <code>RootExtend</code> em AMIs em outros idiomas. Concede permissão de gravação ao grupo de usuários para os arquivos de log. Cria partição MS Reserved para volumes GPT. Adiciona o comando <code>list-volumes</code> e o menu suspenso de volume nas configurações do Amazon EC2Launch. Adiciona comando <code>get-agent-config</code> para imprimir o arquivo <code>agent-config.yaml</code> no formato <code>yaml</code> ou <code>json</code>. Apaga a senha estática se nenhuma chave pública for detectada. 	6 de outubro de 2020
2.0.124	<ul style="list-style-type: none"> Adiciona a opção para exibir a versão do SO no papel de parede. Inicializa volumes criptografados do EBS. Adiciona rotas para VPCs sem nome DNS local. 	10 de setembro de 2020
2.0.104	<ul style="list-style-type: none"> Cria a lista de pesquisa de sufixos DNS, se ela não existir. Ignora a hibernação se não for solicitado. 	12 de agosto de 2020
2.0.0	Versão inicial.	30 de junho de 2020

Histórico de versões da ferramenta de migração do EC2Launch v2

A tabela a seguir descreve as versões lançadas da ferramenta de migração do EC2Launch v2.

Versão	Detalhes	Data de lançamento
1.0.130	Incrementa o número da versão do agente EC2Launch para 2.0.548.	5 de agosto de 2021

Versão	Detalhes	Data de lançamento
1.0.113	Usa IMDSv2 em vez de IMDSv1.	04 de junho de 2021
1.0.101	Incrementa o número da versão do agente EC2Launch para 2.0.285.	12 de março de 2021
1.0.86	Incrementa o número da versão do agente EC2Launch para 2.0.207.	3 de fevereiro de 2021
1.0.76	Incrementa o número da versão do agente EC2Launch para 2.0.160.	4 de dezembro de 2020
1.0.69	Incrementa o número da versão do agente EC2Launch para 2.0.153.	5 de novembro de 2020
1.0.65	Incrementa o número da versão do agente EC2Launch para 2.0.146.	9 de outubro de 2020
1.0.60	Incrementa o número da versão do agente EC2Launch para 2.0.124.	10 de setembro de 2020
1.0.54	<ul style="list-style-type: none">Instala o EC2Launch v2 se nenhum agente estiver instalado.Incrementa o número da versão do agente EC2Launch para 2.0.104.Desacopla o SSM Agent.	12 de agosto de 2020
1.0.50	Remove a dependência do NuGet.	10 de agosto de 2020
1.0.0	Versão inicial.	30 de junho de 2020

Configurar uma instância do Windows usando o EC2Launch

O EC2Launch é um conjunto de scripts do Windows PowerShell que substitui o serviço do EC2Config nas AMIs do Windows Server 2016 e 2019. O Windows Server 2022 usa o [EC2Launch v2 \(p. 482\)](#), o serviço mais recente lançado para todas as versões do Windows compatíveis, que substitui o EC2Config e o EC2Launch.

Tópicos

- [Tarefas do EC2Launch \(p. 523\)](#)
- [Instalar a versão mais recente do EC2Launch \(p. 523\)](#)
- [Verificar a versão do EC2Launch \(p. 524\)](#)
- [Estrutura de diretório do EC2Launch \(p. 524\)](#)
- [Configurar o EC2Launch \(p. 524\)](#)
- [Histórico de versões do EC2Launch \(p. 527\)](#)

Tarefas do EC2Launch

Por padrão, o EC2Launch executa as seguintes tarefas durante a primeira inicialização da instância:

- Configura novo papel de parede que produz informações sobre a instância.
- Define o nome do computador.
- Envia informações da instância ao console do Amazon EC2.
- Envia a impressão digital do certificado RDP ao console do EC2.
- Define uma senha aleatória para a conta do administrador.
- Adiciona sufixos DNS.
- Estende dinamicamente a partição do sistema operacional para incluir qualquer espaço não particionado.
- Executa dados do usuário (se especificado). Para obter mais informações sobre como especificar os dados do usuário, consulte [Trabalhar com dados do usuário da instância \(p. 638\)](#).
- Define rotas estáticas persistentes para alcançar o serviço de metadados e os servidores AWS KMS.

Important

Se uma AMI personalizada for criada a partir dessa instância, essas rotas serão capturadas como parte da configuração do sistema operacional e quaisquer novas instâncias iniciadas a partir da AMI manterão as mesmas rotas, independentemente do posicionamento da sub-rede. Para atualizar as rotas, consulte [Para atualizar rotas de metadados/KMS para o Server 2016 e posterior ao iniciar uma AMI personalizada \(p. 50\)](#).

As seguintes tarefas ajudam a manter a compatibilidade com versões anteriores do serviço do EC2Config. Você também pode configurar o EC2Launch para executar essas tarefas durante o startup:

- Inicializar volumes de EBS secundários.
- Enviar logs de eventos do Windows aos logs do console do EC2.
- Enviar a mensagem O Windows está pronto para uso ao console do EC2.

Para obter mais informações sobre o Windows Server 2019, consulte [Comparar recursos nas versões do Windows Server](#) em Microsoft.com.

Instalar a versão mais recente do EC2Launch

Use o seguinte procedimento para baixar e instalar a versão mais recente do EC2Launch em suas instâncias.

Para fazer download e instalar a versão mais recente do EC2Launch

1. Se você já tiver instalado e configurado o EC2Launch em uma instância, faça um backup do arquivo de configuração do EC2Launch. O processo de instalação não preserva as alterações feitas nesse arquivo. Por padrão, o arquivo está localizado no diretório C:\ProgramData\Amazon\EC2-Windows\Launch\Config.
2. Faça download do [EC2-Windows-Launch.zip](#) em um diretório na instância.
3. Faça download do [install.ps1](#) no mesmo diretório onde você baixou o [EC2-Windows-Launch.zip](#).
4. Executar `install.ps1`
5. Se você fez um backup do arquivo de configuração do EC2Launch, copie-o no diretório C:\ProgramData\Amazon\EC2-Windows\Launch\Config.

Verificar a versão do EC2Launch

Use o comando do Windows PowerShell a seguir para verificar a versão instalada do EC2Launch.

```
PS C:\> Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module\EC2Launch.psd1" | Select Version
```

Estrutura de diretório do EC2Launch

Por padrão, o EC2Launch é instalado nas AMIs do Windows Server 2016 e posterior no diretório raiz C : \ProgramData\Amazon\EC2-Windows\Launch.

Note

Por padrão, o Windows oculta os arquivos e as pastas sob C :\ProgramData. Para visualizar os diretórios e arquivos do EC2Launch, digite o caminho no Windows Explorer ou altere as propriedades da pasta para os arquivos e as pastas ocultos.

O diretório Launch contém os seguintes subdiretórios.

- Scripts — contém os scripts do PowerShell que compõem o EC2Launch.
- Module — contém o módulo para compilação dos scripts relacionados ao Amazon EC2.
- Config — contém arquivos script de configuração que você pode personalizar.
- Sysprep — contém recursos de Sysprep.
- Settings: contém uma aplicação para a interface gráfica do usuário do Sysprep.
- Logs — Contém arquivos de log gerados por scripts.

Todos os diretórios do EC2Launch herdam suas permissões de C :\ProgramData, com exceção do seguinte:

- C :\ProgramData\Amazon\EC2-Windows\Launch\Module\Scripts — Esta pasta herda todas as permissões iniciais de C :\ProgramData quando é criada, mas remove o acesso para usuários normais a CreateFiles no diretório.

Configurar o EC2Launch

Quando a instância tiver sido inicializada pela primeira vez, você pode configurar o EC2Launch para iniciar novamente e executar diferentes tarefas de startup.

Tarefas

- [Configurar as tarefas de inicialização \(p. 524\)](#)
- [Programar o EC2Launch para ser executado em cada inicialização \(p. 525\)](#)
- [Inicializar unidades e mapear as letras de unidades \(p. 526\)](#)
- [Enviar logs de eventos do Windows ao console do EC2 \(p. 527\)](#)
- [Enviar a mensagem O Windows está pronto após uma inicialização bem-sucedida \(p. 527\)](#)

Configurar as tarefas de inicialização

Especifique as configurações no arquivo `LaunchConfig.json` para ativar ou desativar as seguintes tarefas de inicialização:

- Definir o nome do computador.

- Defina o monitor para ficar sempre ligado.
- Configurar novo papel de parede.
- Adicionar a lista de sufixos DNS.
- Estender o tamanho do volume de inicialização.
- Defina a senha de administrador.

Para definir as configurações de inicialização

1. Na instância a ser configurada, abra o seguinte arquivo em um editor de texto: C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json.
2. Atualize as seguintes configurações conforme necessário e salve suas alterações. Forneça uma senha em adminPassword somente se adminPasswordType for Specify.

```
{  
    "setComputerName": false,  
    "setMonitorAlwaysOn": true,  
    "setWallpaper": true,  
    "addDnsSuffixList": true,  
    "extendBootVolumeSize": true,  
    "handleUserData": true,  
    "adminPasswordType": "Random | Specify | DoNothing",  
    "adminPassword": "password that adheres to your security policy (optional)"  
}
```

Os tipos de senha são definidos da seguinte maneira:

Random

O EC2Launch gera uma senha e criptografa-a usando a chave de usuário. O sistema desativa essa configuração depois da execução da instância, portanto, essa senha persistirá se a instância for reinicializada ou parada e iniciada.

Specify

O EC2Launch usa a senha que você especifica adminPassword. Se a senha não atender aos requisitos de sistema, o EC2Launch gera uma senha aleatória. A senha é armazenada em LaunchConfig.json como texto não criptografado e será excluída depois que Sysprep definir a senha do administrador. O EC2Launch criptografa a senha usando a chave de usuário.

DoNothing

O EC2Launch usa a senha que você especifica o arquivo unattend.xml. Se você não especificar uma senha em unattend.xml, a conta de administrador ficará desativada.

3. No Windows PowerShell, execute o seguinte comando para programar a execução do script como uma tarefa agendada do Windows. O script é executado uma vez durante a próxima inicialização e desativa essas tarefas para que não sejam executadas novamente.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -  
Schedule
```

Programar o EC2Launch para ser executado em cada inicialização

Você pode programar o EC2Launch para ser executado em cada inicialização e não apenas na inicialização inicial.

Para programar o EC2Launch para ser executado em cada inicialização:

1. Abra o Windows PowerShell e execute o seguinte comando:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -  
SchedulePerBoot
```

2. Ou execute o executável com o seguinte comando:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

Em seguida, selecione Run EC2Launch on every boot. Você pode especificar que sua instância do EC2 seja Shutdown without Sysprep ou Shutdown with Sysprep.

Note

Quando você habilita o EC2Launch para ser executado em cada inicialização, acontecerá o seguinte na próxima vez que o EC2Launch for executado:

- Se o AdminPasswordType ainda estiver definido como Random, o EC2Launch gerará uma nova senha na próxima inicialização. Após a reinicialização, o AdminPasswordType é automaticamente definido como DoNothing para impedir que o EC2Launch gere novas senhas em inicializações subsequentes. Para evitar que o EC2Launch gere uma nova senha na primeira inicialização, defina manualmente o AdminPasswordType como DoNothing antes de reiniciar.
- HandleUserData será redefinido como false a menos que os dados do usuário tenham persist definido como true. Para obter mais informações sobre scripts de dados, consulte [Scripts de dados de usuário](#) no Guia do usuário do Amazon EC2.

Inicializar unidades e mapear as letras de unidades

Especifique as configurações no arquivo DriveLetterMappingConfig.json para mapear letras de unidades para volumes na instância do EC2. O script inicializa drives que ainda não foram inicializados e particionados.

Para mapear letras de unidade a volumes

1. Abra o arquivo C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json em um editor de textos.
2. Especifique as seguintes configurações de volume e salve suas alterações:

```
{  
  "driveLetterMapping": [  
    {  
      "volumeName": "sample volume",  
      "driveLetter": "H"  
    }  
  ]  
}
```

3. Abra o Windows PowerShell e use o seguinte comando para executar o script do EC2Launch que inicializa os discos:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Para inicializar os discos sempre que a instância for inicializada, adicione o sinalizador –Schedule da seguinte forma:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -Schedule
```

Enviar logs de eventos do Windows ao console do EC2

Especifique configurações no arquivo `EventLogConfig.json` para enviar logs de eventos do Windows aos logs do console do EC2.

Para definir as configurações para enviar logs de eventos do Windows

1. Na instância, abra o arquivo `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` em um editor de texto.
2. Configure as seguintes configurações de registro e salve suas alterações:

```
{
  "events": [
    {
      "logName": "System",
      "source": "An event source (optional)",
      "level": "Error | Warning | Information",
      "numEntries": 3
    }
  ]
}
```

3. No Windows PowerShell, execute o seguinte comando para que o sistema agende o script para execução como uma tarefa agendada do Windows sempre que a instância for inicializada.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -Schedule
```

Os logs podem demorar três minutos ou mais para aparecerem no console do EC2.

Enviar a mensagem O Windows está pronto após uma inicialização bem-sucedida

O serviço de EC2Config envia a mensagem “O Windows está pronto” ao console do EC2 após cada inicialização. O EC2Launch envia essa mensagem somente após a primeira inicialização. Para compatibilidade com versões anteriores do serviço de EC2Config, você pode agendar o EC2Launch para enviar essa mensagem após cada inicialização. Na instância, abra o Windows PowerShell e execute o seguinte comando. O sistema agenda o script para ser executado como uma tarefa agendada do Windows.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -Schedule
```

Histórico de versões do EC2Launch

As AMIs do Windows que são inicializadas com o Windows Server 2016 incluem um conjunto de scripts Windows Powershell chamados EC2Launch. O EC2Launch executa tarefas durante a inicialização inicial da instância. Para obter mais informações sobre as versões do EC2Launch incluídas nas AMIs do Windows, consulte [AWSAMIs do Windows \(p. 29\)](#).

Para fazer download e instalar a versão mais recente do EC2Launch, consulte [Instalar a versão mais recente do EC2Launch \(p. 523\)](#).

A tabela a seguir descreve as versões liberadas do EC2Launch. Observe que o formato da versão foi alterado após a versão 1.3.610.

Versão	Detalhes	Data de lançamento
1.3.2003411	<ul style="list-style-type: none"> Alterou-se a lógica de geração de senha para excluir senhas com baixa complexidade. 	4 de agosto de 2021
1.3.2003364	<ul style="list-style-type: none"> Install-EGPumanager atualizado com suporte a IMDSv2. 	7 de junho de 2021
1.3.2003312	<ul style="list-style-type: none"> Linhas de log adicionadas antes e depois da configuração do parâmetro <code>setMonitorAlwaysOn</code>. Incluída a versão do pacote do AWS Nitro Enclaves no log do console. 	04 de maio de 2021
1.3.2003284	Modelo de permissão aprimorado com atualização do local para armazenar dados do usuário em <code>LocalAppData</code> .	23 de março de 2021
1.3.2003236	<ul style="list-style-type: none"> Método atualizado para definir a senha do usuário em <code>Set-AdminAccount</code> e <code>Randomize-LocalAdminPassword</code>. <code>InitializeDisks</code> fixos para verificar se o disco está definido como somente leitura antes de configurá-lo para gravável. 	11 de fevereiro de 2021
1.3.2003210	Correção de localização para <code>install.ps1</code> .	7 de janeiro de 2021
1.3.2003205	Correção de segurança do <code>install.ps1</code> para atualizar permissões no diretório <code>%ProgramData%AmazonEC2-WindowsLaunchModuleScripts</code> .	28 de dezembro de 2020
1.3.2003189	Adição do <code>w32tm resync</code> depois de adicionar rotas.	4 de dezembro de 2020
1.3.2003155	Informações de tipo de instância atualizadas.	25 de agosto de 2020
1.3.2003150	<code>OsCurrentBuild</code> e <code>OsReleaseId</code> adicionados à saída do console.	22 de abril de 2020
1.3.2003040	Lógica de fallback de versão 1 IMDS corrigida.	7 de abril de 2020
1.3.2002730	Suporte adicionado para IMDS V2.	3 de março de 2020
1.3.2002240	Problemas secundários corrigidos.	31 de outubro de 2019
1.3.2001660	Corrigido o problema de login automático para usuários sem a senha depois da primeira execução do Sysprep.	2 de julho de 2019
1.3.2001360	Problemas secundários corrigidos.	27 de março de 2019
1.3.2001220	Todos os scripts do PowerShell assinados.	28 de fevereiro de 2019
1.3.2001200	Corrigido o problema com <code>InitializeDisks.ps1</code> em que a execução do script em um nó em um Cluster de Failover do Microsoft Windows	27 de fevereiro de 2019

Versão	Detalhes	Data de lançamento
	Server formaria unidades em nós remotos cuja letra da unidade correspondesse à letra da unidade local.	
1.3.2001160	Corrigido o papel de parede ausente no Windows 2019.	22 de fevereiro de 2019
1.3.2001040	<ul style="list-style-type: none"> Plug-in adicionado para configurar o monitor para nunca desligar para corrigir problemas de ACPI. Edição e versão do SQL Server gravadas no console. 	21 de janeiro de 2019
1.3.2000930	Correção para adição de rotas a metadados em ENIs habilitadas para IPv6.	2 de janeiro de 2019
1.3.2000760	<ul style="list-style-type: none"> Configuração padrão para RSS e configurações de fila de recebimento para dispositivos ENA adicionadas Hibernação desabilitada durante Sysprep. 	5 de dezembro de 2018
1.3.2000630	<ul style="list-style-type: none"> Adição da rota 169.254.169.253/32 para servidor DNS. Adicionado filtro de configuração de usuário administrador. Melhorias feitas na hibernação de instâncias. Adicionada opção para programar o EC2Launch para ser executado em cada inicialização. 	9 de novembro de 2018
1.3.2000430.0	<ul style="list-style-type: none"> Rota 169.254.169.123/32 adicionada ao serviço de horário do AMZN. Rota 169.254.169.249/32 adicionada ao serviço de licença do GRID. Adicionado tempo limite de 25 segundos ao tentar iniciar o Systems Manager. 	19 de setembro de 2018
1.3.200039.0	<ul style="list-style-type: none"> Corrigida a letra incorreta de unidade para volumes EBS NVME. Adicionado log adicional para versões do driver NVME. 	15 de agosto de 2018
1.3.2000080	Problemas secundários corrigidos.	
1.3.610	Problema corrigido com redirecionamento de saída e erros para os arquivos de dados do usuário.	
1.3.590	<ul style="list-style-type: none"> Tipos de instâncias ausentes adicionadas ao papel de parede. Problema corrigido com mapeamento de letra de unidade e instalação de disco. 	
1.3.580	<ul style="list-style-type: none"> Get-Metadata corrigido para usar as configurações do proxy do sistema padrão para solicitações da Web. Adicionou um argumento especial para NVMe na inicialização do disco. Problemas secundários corrigidos. 	
1.3.550	Adicionou uma opção <code>-NoShutdown</code> para ativar o Sysprep sem desligamento.	
1.3.540	Problemas secundários corrigidos.	
1.3.530	Problemas secundários corrigidos.	

Versão	Detalhes	Data de lançamento
1.3.521	Problemas secundários corrigidos.	
1.3.0	<ul style="list-style-type: none">Problema de tamanho de hexadecimal corrigido para alteração de nome do computador.Possível loop de reinicialização corrigido para alteração de nome do computador.Problema de configuração de papel de parede corrigido.	
1.2.0	<ul style="list-style-type: none">Atualização para exibir informações sobre o sistema operacional (SO) instalado no log do sistema do EC2.Atualização para exibir a versão do EC2Launch e do SSM Agent no log do sistema do EC2.Problemas secundários corrigidos.	
1.1.2	<ul style="list-style-type: none">Atualização para exibir informações do driver de ENA no log do sistema do EC2.Atualização para excluir o Hyper-V da lógica primária do filtro NIC.O servidor e a porta do AWS KMS foram adicionados à chave do registro para ativação do KMS.Configuração de papel de parede aprimorada para vários usuários.Atualização para limpar rotas no armazenamento persistente.Atualização para remover o z da zona de disponibilidade na lista de sufixos DNS.Atualização para resolver um problema com a tag <runAsLocalSystem> nos dados do usuário.	
1.1.1	Versão inicial.	

Configurar uma instância do Windows usando o serviço EC2Config

O serviço de inicialização mais recente para todas o Windows Server 2022 é o [EC2Launch v2 \(p. 482\)](#), que substitui o EC2Config e o EC2Launch.

As AMIs do Windows para o Windows Server 2012 R2 e anteriores incluem um serviço opcional, o serviço EC2Config (`EC2Config.exe`). O EC2Config é iniciado quando a instância inicia e executa tarefas durante o startup e sempre você iniciar ou para iniciar a instância. O EC2Config também executa tarefas sob demanda. Algumas dessas tarefas são automaticamente habilitadas, enquanto outras precisam ser habilitadas manualmente. Embora opcional, esse serviço dá acesso a recursos avançados que não estariam disponíveis de outra forma. Esse serviço é executado na conta LocalSystem.

Note

O EC2Launch substituiu o EC2Config nas AMIs do Windows para o Windows Server 2016 e 2019. Para obter mais informações, consulte [Configurar uma instância do Windows usando o EC2Launch \(p. 522\)](#). O serviço de inicialização mais recente para todas as versões compatíveis do Windows Server é [EC2Launch v2 \(p. 482\)](#), que substitui o EC2Config e o EC2Launch.

O EC2Config usa arquivos de configurações para controlar sua operação. Você pode atualizar esses arquivos de configurações usando uma ferramenta gráfica ou editando diretamente arquivos XML.

Os arquivos binários de serviço e adicionais estão contidos no diretório %ProgramFiles%\Amazon\EC2ConfigService.

Tópicos

- [Tarefas do EC2Config \(p. 531\)](#)
- [Instalar a versão mais recente do EC2Config \(p. 532\)](#)
- [Interromper, reiniciar, excluir ou desinstalar o EC2Config \(p. 533\)](#)
- [EC2Config e AWS Systems Manager \(p. 534\)](#)
- [EC2Config e Sysprep \(p. 534\)](#)
- [Propriedades do serviço do EC2 \(p. 534\)](#)
- [Arquivos de configurações do EC2Config \(p. 538\)](#)
- [Configure as definições de proxy para o serviço do EC2Config \(p. 542\)](#)
- [Histórico de versões do EC2Config \(p. 544\)](#)
- [Solucionar problemas com o serviço do EC2Config \(p. 558\)](#)

Tarefas do EC2Config

O EC2Config executa tarefas de startup iniciais quando a instância é iniciada pela primeira vez; depois, as desabilita. Para executar novamente essas tarefas, você deve explicitamente habilitá-las antes de fechar a instância ou executar manualmente o Sysprep. Essas tarefas são as seguintes:

- Defina uma senha aleatória e criptografada para a conta do administrador.
- Gerencie e instale o certificado do host usado para abrir a Conexão de Desktop Remoto.
- Estenda dinamicamente a partição do sistema operacional para incluir qualquer espaço não particionado.
- Execute os dados de usuário especificado (e Cloud-Init, se instalado). Para obter mais informações sobre como especificar os dados do usuário, consulte [Trabalhar com dados do usuário da instância \(p. 638\)](#).

O EC2Config executa as tarefas a seguir sempre que a instância for iniciada:

- Altere o nome do host para corresponder ao endereço IP privado na notação Hex (essa tarefa está desabilitada por padrão e deverá ser ativada para execução no início da instância).
- Configure o servidor de gerenciamento de chaves (AWS KMS), verifique o status de ativação do Windows e ative o Windows, conforme necessário.
- Monte todos os volumes do Amazon EBS e volumes de armazenamento de instâncias e mapeie os nomes dos volumes para as letras de unidade.
- Grave entradas do log de eventos no console para ajudar a solucionar problemas (essa tarefa fica desabilitada por padrão e deve ser ativada para execução no início da instância).
- Escreva para o console que o Windows está pronto.
- Adiciona uma rota personalizada para o adaptador de rede primária para habilitar os endereços IP a seguir quando um único NIC ou vários NICs estiverem associados: 169.254.169.250, 169.254.169.251 e 169.254.169.254. Esses endereços são usados pelo Windows Activation e ao acessar metadados de instância.

O EC2Config executa a tarefa a seguir sempre que um usuário faz login:

- Exibe informações do papel de parede do segundo plano do desktop.

Enquanto a instância estiver sendo executada, você pode solicitar que o EC2Config execute a seguinte tarefa sob demanda:

- Executar Sysprep e fechar a instância, de modo que você possa criar as AMIs a partir dela. Para obter mais informações, consulte [Criar uma imagem de máquina da Amazon \(AMI\) padronizada usando o Sysprep \(p. 42\)](#).

Instalar a versão mais recente do EC2Config

Por padrão, o serviço EC2Config está incluído em AMIs anteriores ao Windows Server 2016. Quando o serviço EC2Config for atualizado, as novas AMIs do Windows da AWS incluirão a versão mais recente do serviço. Contudo, você precisa atualizar suas próprias instâncias e AMIs do Windows com a versão mais recente do EC2Config.

Note

O EC2Launch substitui o EC2Config nas AMIs do Windows Server 2016 e 2019. Para obter mais informações, consulte [Configurar uma instância do Windows usando o EC2Launch \(p. 522\)](#). O serviço de inicialização mais recente para todas as versões compatíveis do Windows Server é [EC2Launch v2 \(p. 482\)](#), que substitui o EC2Config e o EC2Launch.

Para obter informações sobre como receber notificações para atualizações do EC2Config, consulte [Assinar as notificações de serviço do EC2Config \(p. 557\)](#). Para obter informações sobre alterações em cada versão, consulte [Histórico de versões do EC2Config \(p. 544\)](#).

Antes de começar

- Verifique que você tem .NET framework 3.5 SP1 ou posterior.
- Por padrão, a configuração substitui os arquivos de configuração durante a instalação e reinicia o serviço EC2Config quando a instalação é concluída. Se você tiver alterado as configurações do serviço EC2Config, copie o arquivo config.xml do diretório %Program Files%\Amazon\Ec2ConfigService\Settings. Após atualizar o serviço EC2Config, você poderá restaurar esse arquivo para reter as alterações nas configurações.
- Se a sua versão do EC2Config for anterior à versão 2.1.19 e você estiver instalando a versão 2.2.12 ou anterior, você deve instalar a versão 2.1.19 primeiro. Para instalar a versão 2.1.19, faça download de [EC2Install_2.1.19.zip](#), descompacte o arquivo e execute EC2Install.exe.

Note

Se a sua versão do EC2Config for anterior à versão 2.1.19 e você estiver instalando a versão 2.3.313 ou posterior, você pode instalá-la diretamente sem instalar a versão 2.1.19 primeiro.

Verificar a versão do EC2Config

Use o procedimento a seguir para verificar a versão do EC2Config que está instalada em suas instâncias.

Para verificar a versão instalada do EC2Config

1. Execute uma instância pela AMI e conecte-se a ela.
2. No Painel de Controle, selecione Programas e Recursos.
3. Na lista de programas instalados, procure Ec2ConfigService. O número da versão aparece na coluna Versão.

Atualizar o EC2Config

Use o seguinte procedimento para fazer download e instalar a versão mais recente do EC2Config em suas instâncias.

Para fazer download e instalar a versão mais recente do EC2Config

1. Faça download e descompacte o [instalador do EC2Config](#).
2. Executar `EC2Install.exe`. Para uma lista completa de opções, execute `EC2Install` com a opção `/?`. Por padrão, a configuração exibe os prompts. Para executar o comando sem prompts, use a opção `/quiet`.

Important

Para manter as configurações personalizadas do arquivo `config.xml` que você salvou, execute `EC2Install` com a opção `/norestart`, restaure as configurações e reinicie o serviço EC2Config manualmente.

3. Se você estiver executando o EC2Config versão 4.0 ou superior, reinicie o SSM Agent na instância do snap-in do Microsoft Services.

Note

As informações da versão atualizada do EC2Config não serão exibidas no log do sistema da instância ou na verificação do Trusted Advisor até que você reinicialize ou interrompa e inicie a instância.

Interromper, reiniciar, excluir ou desinstalar o EC2Config

Você pode gerenciar o serviço EC2Config da mesma forma como qualquer outro serviço.

Para aplicar as configurações atualizadas à sua instância, interrompa e reinicie o serviço. Se você estiver instalando manualmente o EC2Config, deverá primeiro interromper o serviço.

Para interromper o serviço EC2Config

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, selecione Ferramentas Administrativas e clique em Serviços.
3. Na lista de serviços, clique com o botão direito sobre EC2Config e selecione Parar.

Para reiniciar o serviço EC2Config

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, selecione Ferramentas Administrativas e clique em Serviços.
3. Na lista de serviços, clique com o botão direito sobre EC2Config e selecione Reiniciar.

Se você não precisar atualizar as configurações, ao criar sua própria AMI ou usar o AWS Systems Manager, poderá excluir e desinstalar de serviço. A exclusão de um serviço remove a subchave do registro. Desinstalar um serviço elimina os arquivos, a subchave do registro e todos os atalhos do serviço.

Para excluir o serviço EC2Config

1. Inicie uma janela do prompt de comando.
2. Execute o seguinte comando:

```
sc delete ec2config
```

Para desinstalar o EC2Config

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, clique em Painel de Controle.
3. Clique duas vezes em Programas e Recursos.
4. Na lista de programas, selecione EC2ConfigService e clique em Desinstalar.

EC2Config e AWS Systems Manager

O serviço EC2Config processa solicitações de Systems Manager nas instâncias criadas com base em AMIs para versões do Windows Server anteriores ao Windows Server 2016 que foram publicadas antes de novembro de 2016.

Instâncias criadas com base em AMIs para versões do Windows Server anteriores ao Windows Server 2016, publicadas depois de novembro de 2016 incluem o serviço EC2Config e SSM Agent. O EC2Config executa todas as tarefas descritas anteriormente e o SSM Agent processa recursos do Systems Manager, como Run Command e o State Manager.

Você pode usar Run Command para atualizar suas instâncias existentes e usar a versão mais recente do serviço EC2Config e do SSM Agent. Para obter mais informações, consulte [Update SSM Agent by using Run Command](#) (Atualizar o SSM Agent usando o Run Command) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).

EC2Config e Sysprep

O serviço EC2Config executa o Sysprep, uma ferramenta da Microsoft que permite a criação de uma AMI personalizada do Windows que pode ser reutilizada. Quando o EC2Config acessa o Sysprep, ela usa os arquivos em %ProgramFiles%\Amazon\EC2ConfigService\Settings para determinar quais operações devem ser executadas. Você pode editar esses arquivos indiretamente usando a caixa de diálogo Propriedades do Serviço Ec2 ou diretamente usando um editor de XML ou de texto. Contudo, há algumas configurações avançadas que não estão disponíveis na caixa de diálogo Propriedades do serviço Ec2; portanto, você deve editar as entradas diretamente.

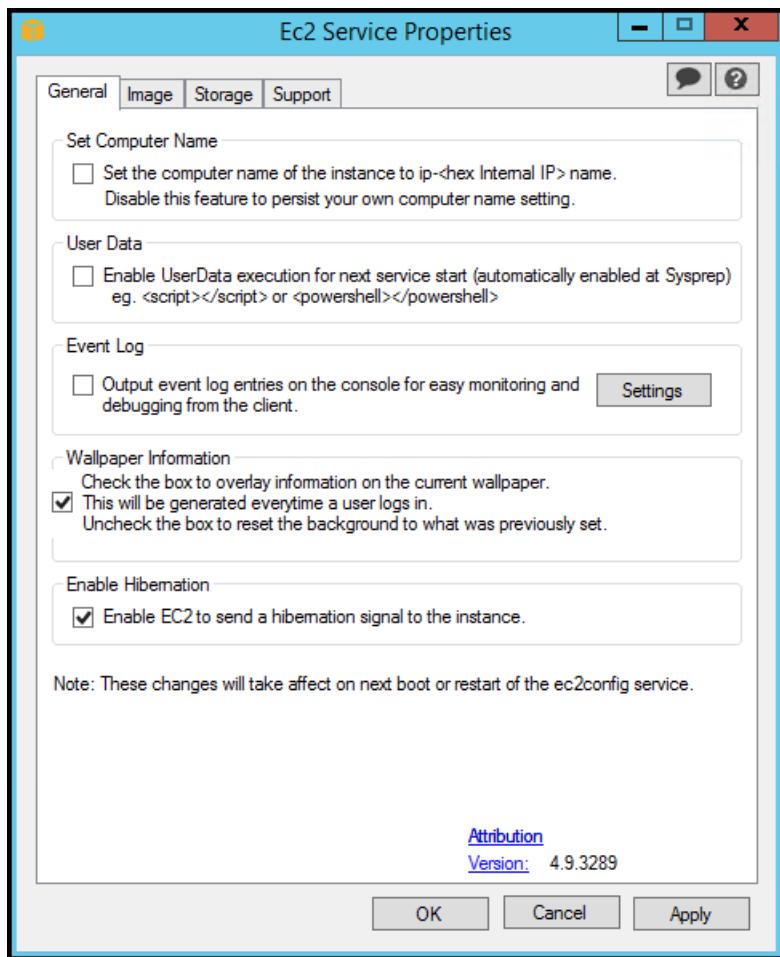
Se você criar AMIs com base em uma instância depois de atualizar suas configurações, as configurações novas serão aplicadas a qualquer instância executada pela nova AMI. Para obter informações sobre como criar uma AMI, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#).

Propriedades do serviço do EC2

O procedimento a seguir descreve como usar a caixa de diálogo Propriedades do serviço Ec2 para permitir ou desabilitar configurações.

Para alterar as configurações usando a caixa de diálogo Propriedades do serviço Ec2

1. Execute e conecte-se à sua instância do Windows.
2. No menu Iniciar, clique em Todos os programas e escolha Configurações do EC2ConfigService.



3. Na guia Geral da caixa de diálogo Propriedades do serviço Ec2, você pode habilitar ou desabilitar as configurações a seguir.

Definir o nome do computador

Se essa configuração estiver habilitada (está desabilitada por padrão), o nome do host será comparado ao endereço IP interno atual a cada inicialização; se o nome de host e o endereço IP interno não corresponderem, o nome do host será redefinido para conter o endereço IP interno, e o sistema reiniciará para pegar o novo nome de host. Ao configurar seu próprio nome de host ou para impedir a modificação de um nome de host existente, não habilite essa configuração.

Dados do usuário

A execução de dados do usuário permite especificar scripts nos metadados da instância. Por padrão, esses scripts são executados durante a execução inicial. Também é possível configurá-los para que sejam executados na próxima vez que você reiniciar ou iniciar a instância, ou sempre que fizer esse procedimento.

Se você tem um script grande, recomendamos usar dados do usuário para fazer download do script e, em seguida, executá-lo.

Para obter mais informações, consulte [Execução de dados do usuário \(p. 616\)](#).

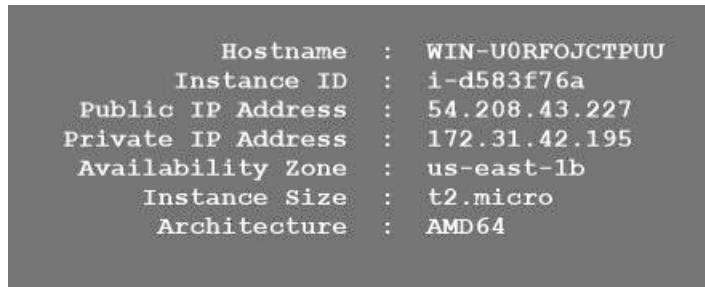
Log de eventos

Use essa configuração para exibir entradas de log de eventos no console durante a inicialização para facilitar o monitoramento e a depuração.

Clique em Configurações para especificar filtros para as entradas do log enviadas ao console. O filtro padrão enviar as três entradas de erros mais recentes do log de eventos do sistema ao console.

Informações sobre o papel de parede

Use essa configuração para exibir informações do sistema no segundo plano do desktop. A seguir está um exemplo das informações exibidas na tela de fundo do desktop.



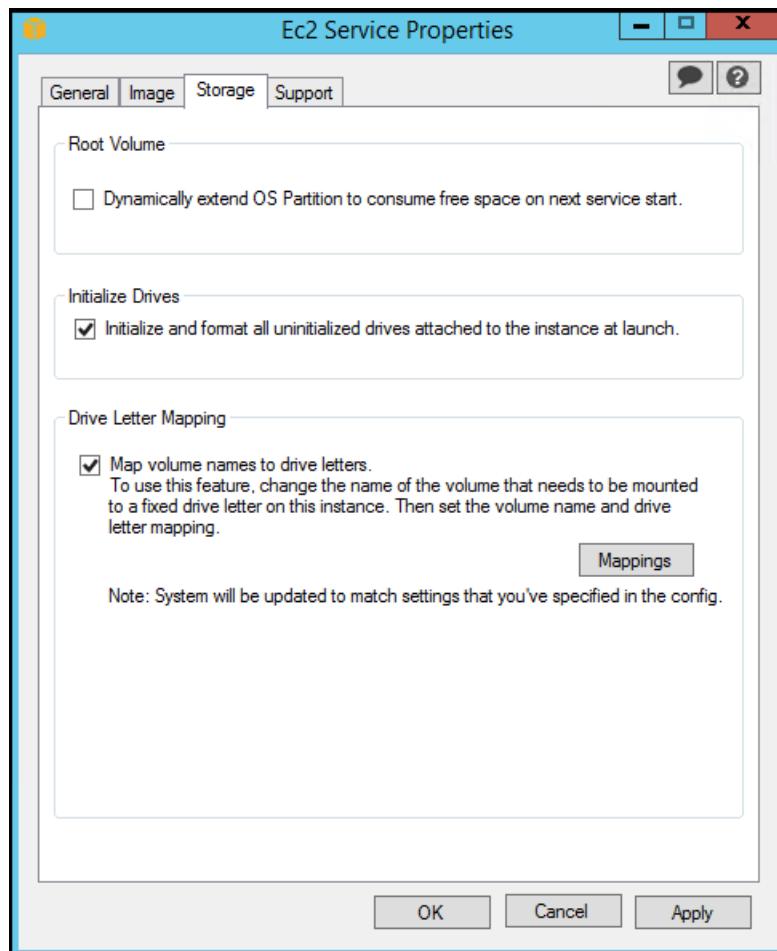
```
Hostname      : WIN-U0RFOJCTPUU
Instance ID   : i-d583f76a
Public IP Address : 54.208.43.227
Private IP Address : 172.31.42.195
Availability Zone : us-east-1b
Instance Size   : t2.micro
Architecture    : AMD64
```

As informações exibidas em segundo plano no desktop são controladas pelo arquivo de configurações EC2ConfigService\Settings\WallpaperSettings.xml.

Enable Hibernation (Habilitar a hibernação)

Use essa configuração para permitir que o EC2 sinalize ao sistema operacional para executar a hibernação.

4. Clique na guia Armazenamento. Você pode habilitar ou desabilitar as configurações a seguir.



Volume do dispositivo raiz

Essa configuração amplia dinamicamente o Disco 0/Volume 0 para incluir qualquer espaço não particionado. Isso pode ser útil quando a instância for inicializada a partir de um volume do dispositivo raiz com tamanho personalizado.

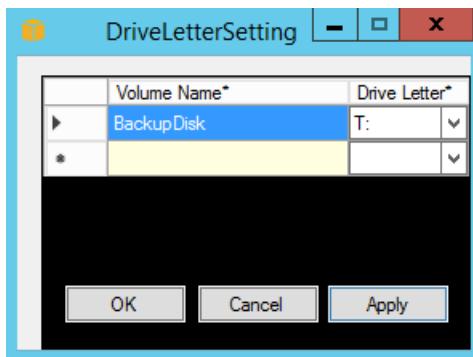
Iniciar unidades

Essa configuração formata e monta todos os volumes associados à instância durante a inicialização.

Mapeamento da letra da unidade

O sistema mapeia os volumes associados a uma instância para as letras de unidade. Para volumes do Amazon EBS, o padrão é atribuir letras de unidade que vão de D: a Z:. Para volumes de armazenamento de instâncias, o padrão depende do driver. AWS Os drivers PV e Citrix PV atribuem aos volumes de armazenamento de instância letras que vão de Z: a A:. Os drivers do Red Hat atribuem aos volumes de armazenamento da instância letras de unidades que vão de D: a Z:.

Para selecionar as letras de unidade para seus volumes, clique em Mapeamentos. Na caixa de diálogo DriveLetterSetting, especifique os valores de Volume Name (Nome do volume) e Drive Letter (Letra da unidade) para cada volume e clique em Apply (Aplicar) e, em seguida, OK. Recomendamos que você selecione letras de unidade que evitem conflitos com as letras de unidade que provavelmente estão em uso, como as do meio do alfabeto.



Após especificar um mapeamento de letra de unidade e associar um volume com o mesmo rótulo que um dos nomes de volume especificado, o EC2Config atribui automaticamente sua letra especificada para esse volume. Contudo, o mapeamento da letra de unidade falhará se a letra já estiver em uso. Observe que EC2Config não altera as letras de unidade dos volumes já montados ao especificar o mapeamento da letra de unidade.

5. Para salvar suas configurações e continuar trabalhando nelas depois, clique em OK para fechar a caixa de diálogo Propriedades do serviço Ec2. Se você tiver concluído a personalização da sua instância e quiser criar uma AMI com base nessa instância, consulte [Criar uma imagem de máquina da Amazon \(AMI\) padronizada usando o Sysprep \(p. 42\)](#).

Arquivos de configurações do EC2Config

Os arquivos de configurações controlam a operação do serviço EC2Config. Esses arquivos estão localizados no diretório C:\Program Files\Amazon\Ec2ConfigService\Settings:

- ActivationSettings.xml—Controla a ativação do produto usando um servidor de gerenciamento de chaves (AWS KMS).
- AWS.EC2.Windows.CloudWatch.json: controla quais contadores de performance enviar ao CloudWatch e quais logs enviar ao CloudWatch Logs.
- BundleConfig.xml—Controla como o EC2Config prepara uma instância com armazenamento de instâncias para criação da AMI.
- Config.xml—Controla as configurações primárias.
- DriveLetterConfig.xml—Controla os mapeamentos da letra de unidade.
- EventLogConfig.xml—Controla as informações do log de eventos exibidas no console enquanto a instância está inicializando.
- WallpaperSettings.xml—Controla as informações exibidas na tela de fundo do desktop.

ActivationSettings.xml

Esse arquivo contém as configurações que controlam a ativação do produto. Quando o Windows inicializa, o serviço EC2Config verifica se o Windows já está ativado. Se o Windows ainda não estiver ativado, ele tentará ativar o Windows procurando pelo servidor AWS KMS específico.

- SetAutodiscover: indica se é necessário detectar um AWS KMS automaticamente.
- TargetKMSServer—Armazena o endereço IP privado de um AWS KMS. O AWS KMS deve estar na mesma região que a instância.
- DiscoverFromZone: descobre o servidor AWS KMS da zona de DNS especificada.
- ReadFromUserData: obtém o servidor AWS KMS de UserData.

- **LegacySearchZones**: descobre o servidor AWS KMS da zona de DNS especificada.
- **DoActivate**—Tenta a ativação usando as configurações especificadas na seção. Esse valor pode ser **true** ou **false**.
- **LogResultToConsole**—Exibe o resultado para o console.

BundleConfig.xml

Este arquivo contém configurações que controlam como o EC2Config prepara uma instância para criação da AMI.

- **AutoSysprep**—Indica se o Sysprep deve ser usado automaticamente. Altere o valor para **Yes** para usar o Sysprep.
- **SetRDP Certificate**: define um certificado autoassinado para o servidor de Desktop Remoto. Isso permite que você use RDP com segurança nas instâncias. Altere o valor para **Yes** se as novas instâncias precisarem ter o certificado.

Essa configuração não é usada com instâncias do Windows Server 2008 ou Windows Server 2012, pois podem gerar seus próprios certificados.

- **SetPasswordAfterSysprep**—Define uma senha aleatória em uma instância recém-executada, criptografa-a com a chave de execução do usuário e gera a senha criptografada no console. Altere o valor dessa configuração para **No** se as novas instâncias não forem definidas como uma senha criptografada aleatória.

Config.xml

Plug-ins

- **Ec2SetPassword**—Gera uma senha criptografada aleatória sempre que você executar uma instância. Esse recurso é desabilitado por padrão após a primeira execução, de forma que as reinicializações dessa instância não alterem uma senha definida pelo usuário. Altere essa configuração para **Enabled** para continuar a gerar senhas sempre que você executar uma instância.

Essa configuração é importante se você estiver planejando criar um AMI a partir da sua instância.

- **Ec2SetComputerName**—Define o nome do host da instância para um nome exclusivo baseado no endereço IP da instância e reinicia a instância. Ao configurar seu próprio nome de host ou impedir a modificação de um nome de host existente, é preciso desabilitar essa configuração.
- **Ec2InitializeDrives**—Inicializa e formata todos os volumes durante o startup. Esse recurso está habilitado por padrão.
- **Ec2EventLog**—Exibe entradas no log de eventos do console. Por padrão, são exibidas as três entradas de erro mais recentes do log de eventos do sistema. Para especificar as entradas no log de evento a serem exibidas, edite o arquivo `EventLogConfig.xml` localizado no diretório `EC2ConfigService\Settings`. Para obter informações sobre as configurações nesse arquivo, consulte [Eventlog Key](#) na biblioteca do MSDN.
- **Ec2ConfigureRDP**—Define um certificado autoatribuído na instância, de forma que os usuários possam acessar com segurança a instância usando o Desktop Remoto. Esse recurso é desabilitado nas instâncias do Windows Server 2008 e do Windows Server 2012, pois podem gerar seus próprios certificados.
- **Ec2OutputRDPCert**—Exibe informações do certificado de Desktop Remoto ao console, de forma que o usuário possa verificá-las contra o thumbprint.
- **Ec2SetDriveLetter**—Define as letras de unidade dos volumes montados com base em configurações definidas pelo usuário. Por padrão, quando um volume do Amazon EBS estiver associado a uma instância, ele poderá ser montado usando a letra de unidade na instância. Para especificar os mapeamentos da sua letra de unidade, edite o arquivo `DriveLetterConfig.xml` localizado no diretório `EC2ConfigService\Settings`.

- **Ec2WindowsActivate**— O plug-in lida com ativação do Windows. Verifica para ver se o Windows está ativado. Caso contrário, atualiza as configurações do cliente AWS KMS e, então, ativa o Windows.

Para modificar as configurações do AWS KMS, edite o arquivo `ActivationSettings.xml` localizado no diretório `EC2ConfigService\Settings`.

- **Ec2DynamicBootVolumeSize**—Estende o disco 0/Volume 0 para incluir qualquer espaço não particionado.
- **Ec2HandleUserData**—Cria e executa scripts criados pelo usuário na primeira execução de uma instância depois que o Sysprep for executado. Os comandos envolvidos nas tag do script são gravados no arquivo em lote, e os comandos envolvidos nas tags do PowerShell são gravados em um arquivo .ps1 (corresponde à caixa de seleção User Data [Dados do usuário] na caixa de diálogo Ec2 Service Properties [Propriedades do serviço Ec2]).
- **Ec2ElasticGpuSetup**—Instala o pacote de software para GPU elástica se a instância estiver associada a uma GPU elástica.
- **Ec2FeatureLogging**—Envia a instalação do recurso do Windows e o status do serviço correspondente ao console. Suportado somente para o recurso Microsoft Hyper-V e o serviço vmms correspondente.

Configurações globais

- **ManageShutdown**—Assegura que as instâncias executadas pelas AMIs com armazenamento de instâncias não sejam encerradas ao executar Sysprep.
- **SetDnsSuffixList**—Define o sufixo DNS do adaptador de rede para Amazon EC2. Isso permite resolução do DNS dos servidores em execução no Amazon EC2 sem fornecer o nome de domínio totalmente qualificado.
- **WaitForMetaDataAvailable**—Assegura que o serviço EC2Config aguardará os metadados estarem acessíveis e redes estarem disponíveis antes de continuar com a inicialização. Essa verificação garante que o EC2Config possa obter informações dos metadados para ativação e outros plug-ins.
- **ShouldAddRoutes**—Adiciona uma rota personalizada para o adaptador de rede primária para habilitar os endereços IP a seguir quando múltiplos NICs estiverem associados: 169.254.169.250, 169.254.169.251 e 169.254.169.254. Esses endereços são usados pelo Windows Activation e ao acessar metadados de instância.
- **RemoveCredentialsFromSysprepOnStartup**—Remove a senha do administrador de `Sysprep.xml` da próxima vez que o serviço iniciar. Para garantir que essa senha persista, edite essa configuração.

DriveLetterConfig.xml

Esse arquivo contém configurações que controlam os mapeamentos de letra da unidade. Por padrão, um volume pode ser mapeado para qualquer letra de unidade disponível. Você pode montar um volume em uma letra de unidade específica, da seguinte forma.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
  .
  .
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- **VolumeName**—A etiqueta de volume. Por exemplo, *My Volume*. Para especificar um mapeamento para um volume de armazenamento de instâncias, use a etiqueta **Temporary Storage X**, onde X é um número de 0 a 25.
- **DriveLetter**—A letra de unidade. Por exemplo, *M:*. O mapeamento falhará se a letra de unidade já estiver em uso.

EventLogConfig.xml

Este arquivo contém configurações que controlam as informações do log de eventos exibidas no console enquanto a instância estiver sendo inicializada. Por padrão, exibimos as três entradas de erro mais recentes do log de eventos do sistema.

- **Category**—A chave de log do evento a ser monitorada.
- **ErrorType**—O tipo de evento (por exemplo, **Error**, **Warning**, **Information**.)
- **NumEntries**—O número de eventos armazenados para essa categoria.
- **LastMessageTime**—Para impedir que a mesma mensagem seja enviada repetidamente, o serviço atualizará esse valor sempre que enviar uma mensagem.
- **AppName**: a origem do evento ou a aplicação que o registrou.

WallpaperSettings.xml

Esse arquivo contém as configurações que controlam as informações exibidas na tela de fundo do desktop. As informações a seguir são exibidas por padrão.

- **Hostname**—Exibe o nome do computador.
- **Instance ID**—Exibe o ID da instância.
- **Public IP Address**—Exibe o endereço IP público da instância.
- **Private IP Address**—Exibe o endereço IP privado da instância.
- **Availability Zone**—Exibe a zona de disponibilidade na qual a instância está em execução.
- **Instance Size**—Exibe o tipo de instância.
- **Architecture**—Exibe a configuração da variável de ambiente **PROCESSOR_ARCHITECTURE**.

Você pode remover qualquer informação exibida por padrão ao excluir essa entrada. Você pode adicionar metadados de instância adicionais para exibir da forma a seguir.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

Você pode adicionar variáveis do ambiente do sistema para exibir da forma a seguir.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Esse arquivo contém as configurações que controlam como o EC2Config inicializa as unidades.

Por padrão, o EC2Config inicializa as unidades que não foram trazidas online com o sistema operacional. Você pode personalizar o plug-in conforme a seguir.

```
<InitializeDrivesSettings>
  <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Use um grupo de configurações para especificar como deseja inicializar as unidades:

FormatWithTRIM

Permite o comando TRIM ao formatar as unidades. Após uma unidade ser formatada e inicializada, o sistema restaurará a configuração de TRIM.

A partir do EC2Config versão 3.18, o comando TRIM é desativado durante a operação de formatação do disco, por padrão. Isso aprimora o tempo de formatação. Use essa configuração para permitir a TRIM durante a operação de formatação do disco para o EC2Config versão 3.18 e posterior.

FormatWithoutTRIM

Desabilita o comando TRIM ao formatar as unidades e melhorar o tempo de formatação no Windows. Após uma unidade ser formatada e inicializada, o sistema restaurará a configuração de TRIM.

DisableInitializeDrives

Desabilita a formatação de novas unidades. Use essa configuração para inicializar as unidades manualmente.

Configure as definições de proxy para o serviço do EC2Config

Você pode configurar o serviço EC2Config para se comunicar por meio de um proxy usando um dos seguintes métodos: AWS SDK for .NET, o elemento `system.net` as políticas de grupo da Microsoft e o Internet Explorer. O AWS SDK for .NET é o método preferido, pois você pode especificar um nome e uma senha de usuário.

Métodos

- [Configurar definições de proxy usando a opção AWS SDK for .NET \(Preferencial\) \(p. 542\)](#)
- [Definir as configurações de proxy usando o elemento system.net \(p. 543\)](#)
- [Definir as configurações de proxy usando as políticas do grupo Microsoft e o Internet Explorer \(p. 543\)](#)

Configurar definições de proxy usando a opção AWS SDK for .NET (Preferencial)

Você pode configurar as configurações de proxy para o serviço EC2Config ao especificar o elemento `proxy` no arquivo `Ec2Config.exe.config`. Para obter mais informações, consulte [Referência de arquivos de configuração do AWS SDK for .NET](#).

Para especificar o elemento de proxy em `Ec2Config.exe.config`

1. Edite o arquivo `Ec2Config.exe.config` em uma instância onde deseja que o serviço EC2Config se comunica através de um proxy. Por padrão, o arquivo está localizado no seguinte diretório:
`%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Adicione o elemento `aws` a seguir para o `configSections`. Não adicione isso a nenhum `sectionGroups` existente.

Para EC2Config versões 3.17 ou anteriores

```
<configSections>
```

```
<section name="aws" type="Amazon.AWSSection, AWSSDK"/>  
</configSections>
```

Para EC2Config versões 3.18 ou posteriores

```
<configSections>  
    <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>  
</configSections>
```

3. Adicione o elemento aws a seguir ao arquivo Ec2Config.exe.config.

```
<aws>  
    <proxy  
        host="string value"  
        port="string value"  
        username="string value"  
        password="string value" />  
</aws>
```

4. Salve as alterações.

Definir as configurações de proxy usando o elemento system.net

Você pode especificar as configurações de proxy em um elemento system.net no arquivo Ec2Config.exe.config. Para obter mais informações, consulte o [elemento defaultProxy \(configurações de rede\)](#) em MSDN.

Para especificar o elemento system.net em Ec2Config.exe.config

1. Edite o arquivo Ec2Config.exe.config em uma instância onde deseja que o serviço EC2Config se comunica através de um proxy. Por padrão, o arquivo está localizado no seguinte diretório: %ProgramFiles%\Amazon\Ec2ConfigService.
2. Adicione uma entrada defaultProxy a system.net. Para obter mais informações, consulte o [elemento defaultProxy \(configurações de rede\)](#) em MSDN.

Por exemplo, a configuração a seguir roteia todo o tráfego para usar o proxy atualmente configurado para Internet Explorer, com exceção de metadados e tráfego de licenciamento, que contorneará o proxy.

```
<defaultProxy>  
    <proxy usesystemdefault="true" />  
    <bypasslist>  
        <add address="169.254.169.250" />  
        <add address="169.254.169.251" />  
        <add address="169.254.169.254" />  
    </bypasslist>  
</defaultProxy>
```

3. Salve as alterações.

Definir as configurações de proxy usando as políticas do grupo Microsoft e o Internet Explorer

O serviço EC2Config é executado sob a conta do usuário do sistema local. Você pode especificar configurações de proxy em toda a instância para essa conta no Internet Explorer depois de alterar as configurações de Política do Grupo na instância.

Para definir as configurações de proxy usando as políticas de grupo e o Internet Explorer

1. Em uma instância na qual você deseja que o serviço EC2Config se comunique por um proxy, abra um prompt de comando como administrador, digite **gpedit.msc** e pressione Enter.
2. No editor de políticas do grupo local, em Política do computador local, escolha Configuração do computador, Modelos administrativos, Componentes do Windows, Internet Explorer.
3. No painel à direita, escolha Definir as configurações de proxy por máquina (não por usuário) e, em seguida, Editar configuração da política.
4. Selecione Habilitado e, em seguida, selecione Aplicar.
5. Abra o Internet Explorer e selecione o botão Ferramentas.
6. Escolha Opção de Internet e escolha a guia Conexões.
7. Escolha Configurações da LAN.
8. Em Servidor proxy, escolha a opção Usar um Servidor Proxy para LAN.
9. Especifique as informações de endereço e porta e selecione OK.

Histórico de versões do EC2Config

As AMIs do Windows antes do Windows Server 2016 incluem um serviço opcional chamado serviço EC2Config (`EC2Config.exe`). O EC2Config é iniciado quando a instância inicia e executa tarefas durante o startup e sempre você iniciar ou para iniciar a instância. Para obter mais informações sobre as versões do EC2Config incluídas nas AMIs do Windows, consulte [AWSAMIs do Windows \(p. 29\)](#).

Você pode receber notificações quando novas versões do serviço EC2Config forem liberadas. Para obter mais informações, consulte [Assinar as notificações de serviço do EC2Config \(p. 557\)](#).

A tabela a seguir descreve as versões liberadas do EC2Config. Para obter informações sobre as atualizações do SSM Agent, consulte [Notas de release do Systems Manager SSM Agent](#).

Versão	Detalhes	Data de lançamento
4.9.4500	<ul style="list-style-type: none">• <code>Install-EgpuManagerConfig</code> atualizado com suporte a IMDS v2.• Links atualizados para usar https.• Nova versão do SSM Agent 3.1.282.0	7 de setembro de 2021
4.9.4419	<ul style="list-style-type: none">• Lógica de fallback de versão 1 IMDS corrigida.• Atualizado todo o uso do diretório temporário do Windows para o diretório temporário do EC2Config• Nova versão do SSM Agent 3.0.1124.0	2 de junho de 2021
4.9.4381	<ul style="list-style-type: none">• Adicionado suporte para o esquema de documentos SSM versão 2.2 no EC2ConfigUpdater• Incluída a versão do pacote do AWS Nitro Enclaves no log do console• Nova versão do SSM Agent 3.0.529.0	4 de maio de 2021
4.9.4326	<ul style="list-style-type: none">• Todos os links na interface do usuário de configurações foram removidos• Esta é a última versão do EC2Config que oferece suporte ao Windows Server 2008.	3 de março de 2021

Versão	Detalhes	Data de lançamento
4.9.4279	<ul style="list-style-type: none"> Corrigido problema de segurança relacionado à tarefa <code>Ec2ConfigMonitor</code> agendada Corrigido problema de mapeamento de letras de unidade fixa e contagem de disco temporário incorreta Adicionados <code>OsCurrentBuild</code> e <code>OsReleaseId</code> à saída do console. Nova versão do SSM Agent 2.3.871.0 	11 de dezembro de 2020
4.9.4222	<ul style="list-style-type: none"> Lógica de fallback de versão 1 IMDS corrigida. Nova versão do SSM Agent 2.3.842.0 	7 de abril de 2020
4.9.4122	<ul style="list-style-type: none"> Supporte adicionado para IMDS v2 Nova versão do SSM Agent 2.3.814.0 	4 de março de 2020
4.9.3865	<ul style="list-style-type: none"> Correção de um problema que detecta a porta COM para Windows Server 2008 R2 em instâncias metal Nova versão do SSM Agent 2.3.722.0 	31 de outubro de 2019
4.9.3519	<ul style="list-style-type: none"> Nova versão do SSM Agent 2.3.634.0 	18 de junho de 2019
4.9.3429	<ul style="list-style-type: none"> Nova versão do SSM Agent 2.3.542.0 	25 de abril de 2019
4.9.3289	<ul style="list-style-type: none"> Nova versão do SSM Agent 2.3.444.0 	11 de fevereiro de 2019
4.9.3270	<ul style="list-style-type: none"> Plug-in adicionado a fim de configurar o monitor para nunca desligar ao corrigir problemas de ACPI Edição e versão do SQL Server gravadas no console Nova versão do SSM Agent 2.3.415.0 	22 de janeiro de 2019
4.9.3230	<ul style="list-style-type: none"> A descrição do Mapeamento da letra da unidade foi atualizada para se alinhar melhor à funcionalidade. Nova versão do SSM Agent 2.3.372.0 	10 de janeiro de 2019
4.9.3160	<ul style="list-style-type: none"> Aumentado o tempo de espera para NIC primário Adição de configuração padrão para RSS e configurações de fila de recebimento para dispositivos ENA Hibernação desabilitada durante Sysprep Nova versão do SSM Agent 2.3.344.0 AWS SDK atualizado para 3.3.29.13 	15 de dezembro de 2018
4.9.3067	<ul style="list-style-type: none"> Melhorias feitas na hibernação de instâncias Nova versão do SSM Agent 2.3.235.0 	8 de novembro de 2018
4.9.3034	<ul style="list-style-type: none"> Adição da rota 169.254.169.253/32 para servidor DNS Nova versão do SSM Agent 2.3.193.0 	24 de outubro de 2018
4.9.2986	<ul style="list-style-type: none"> Adição de assinatura para todos os binários relacionados ao EC2Config Nova versão do SSM Agent 2.3.136.0 	11 de outubro de 2018

Versão	Detalhes	Data de lançamento
4.9.2953	Nova versão do SSM Agent (2.3.117.0)	2 de outubro de 2018
4.9.2926	Nova versão do SSM Agent (2.3.68.0)	18 de setembro de 2018
4.9.2905	<ul style="list-style-type: none"> • Nova versão do SSM Agent (2.3.50.0) • Rota 169.254.169.123/32 adicionada ao serviço de horário do AMZN • Rota 169.254.169.249/32 adicionada ao serviço de licença do GRID • Corrigido um problema que fazia com que os volumes do EBS NVMe fossem marcados como efêmeros 	17 de setembro de 2018
4.9.2854	Nova versão do SSM Agent (2.3.13.0)	17 de agosto de 2018
4.9.2831	Nova versão do SSM Agent (2.2.916.0)	7 de agosto de 2018
4.9.2818	Nova versão do SSM Agent (2.2.902.0)	31 de julho de 2018
4.9.2756	Nova versão do SSM Agent (2.2.800.0)	27 de junho de 2018
4.9.2688	Nova versão do SSM Agent (2.2.607.0)	25 de maio de 2018
4.9.2660	Nova versão do SSM Agent (2.2.546.0)	11 de maio de 2018
4.9.2644	Nova versão do SSM Agent (2.2.493.0)	26 de abril de 2018
4.9.2586	Nova versão do SSM Agent (2.2.392.0)	28 de março de 2018
4.9.2565	<ul style="list-style-type: none"> • Nova versão do SSM Agent (2.2.355.0) • Foi corrigido um problema nas instâncias M5 e C5 (não conseguem encontrar os drivers PV) • Adicionado o registro em log no console para tipo de instância, drivers PV mais recentes e drivers NVMe 	13 de março de 2018
4.9.2549	Nova versão do SSM Agent (2.2.325.0)	8 de março de 2018
4.9.2461	Nova versão do SSM Agent (2.2.257.0)	15 de fevereiro de 2018
4.9.2439	Nova versão do SSM Agent (2.2.191.0)	6 de fevereiro de 2018
4.9.2400	Nova versão do SSM Agent (2.2.160.0)	16 de janeiro de 2018

Versão	Detalhes	Data de lançamento
4.9.2327	<ul style="list-style-type: none"> Nova versão do SSM Agent (2.2.120.0) Descoberta de porta COM adicionada em instâncias bare metal do Amazon EC2 Registro em log de status Hyper-V adicionado em instâncias bare metal do Amazon EC2 	2 de janeiro de 2018
4.9.2294	Nova versão do SSM Agent (2.2.103.0)	4 de dezembro de 2017
4.9.2262	Nova versão do SSM Agent (2.2.93.0)	15 de novembro de 2017
4.9.2246	Nova versão do SSM Agent (2.2.82.0)	11 de novembro de 2017
4.9.2218	Nova versão do SSM Agent (2.2.64.0)	29 de outubro de 2017
4.9.2212	Nova versão do SSM Agent (2.2.58.0)	23 de outubro de 2017
4.9.2203	Nova versão do SSM Agent (2.2.45.0)	19 de outubro de 2017
4.9.2188	Nova versão do SSM Agent (2.2.30.0)	10 de outubro de 2017
4.9.2180	<ul style="list-style-type: none"> Nova versão do SSM Agent (2.2.24.0) Plugin de GPU elástica adicionado a instâncias de GPU 	5 de outubro de 2017
4.9.2143	Nova versão do SSM Agent (2.2.16.0)	1º de outubro de 2017
4.9.2140	Nova versão do SSM Agent (2.1.10.0)	
4.9.2130	Nova versão do SSM Agent (2.1.4.0)	
4.9.2106	Nova versão do SSM Agent (2.0.952.0)	
4.9.2061	Nova versão do SSM Agent (2.0.922.0)	
4.9.2047	Nova versão do SSM Agent (2.0.913.0)	
4.9.2031	Nova versão do SSM Agent (2.0.902.0)	
4.9.2016	<ul style="list-style-type: none"> Nova versão do SSM Agent (2.0.879.0) Caminho do diretório do CloudWatch Logs corrigido para o Windows Server 2003 	
4.9.1981	<ul style="list-style-type: none"> Nova versão do SSM Agent (2.0.847.0) Corrigido o problema com <code>important.txt</code> sendo gerado em volumes do EBS. 	
4.9.1964	Nova versão do SSM Agent (2.0.842.0)	

Versão	Detalhes	Data de lançamento
4.9.1951	<ul style="list-style-type: none"> Nova versão do SSM Agent (2.0.834.0) Corrigido o problema com letra de unidade não mapeada de Z: para discos temporários. 	
4.9.1925	<ul style="list-style-type: none"> Nova versão do SSM Agent (2.0.822.0) [Bug] Essa versão não é um destino de atualização válido do SSM Agent v4.9.1775. 	
4.9.1900	Nova versão do SSM Agent (2.0.805.0)	
4.9.1876	<ul style="list-style-type: none"> Nova versão do SSM Agent (2.0.796.0) Corrigido um problema com redirecionamento de saída/erro para execução de userdata do administrador. 	
4.9.1863	<ul style="list-style-type: none"> Nova versão do SSM Agent (2.0.790.0) Corrigidos problemas com a conexão de vários volumes do EBS a uma instância do Amazon EC2. Melhorado o CloudWatch para pegar um caminho de configuração, mantendo a retrocompatibilidade. 	
4.9.1791	Nova versão do SSM Agent (2.0.767.0)	
4.9.1775	Nova versão do SSM Agent (2.0.761.0)	
4.9.1752	Nova versão do SSM Agent (2.0.755.0)	
4.9.1711	Nova versão do SSM Agent (2.0.730.0)	
4.8.1676	Nova versão do SSM Agent (2.0.716.0)	
4.7.1631	Nova versão do SSM Agent (2.0.682.0)	
4.6.1579	<ul style="list-style-type: none"> Nova versão do SSM Agent (2.0.672.0) Corrigido problema de atualização do agente com v4.3, v4.4 e v4.5 	
4.5.1534	Nova versão do SSM Agent (2.0.645.1)	
4.4.1503	Nova versão do SSM Agent (2.0.633.0)	
4.3.1472	Nova versão do SSM Agent (2.0.617.1)	
4.2.1442	Nova versão do SSM Agent (2.0.599.0)	
4.1.1378	Nova versão do SSM Agent (2.0.558.0)	

Versão	Detalhes	Data de lançamento
4.0.1343	<ul style="list-style-type: none"> O Run Command, o State Manager, o agente do CloudWatch e o suporte à união de domínios foram transferidos para outro agente, chamado SSM Agent. O SSM Agent será instalado como parte do upgrade do EC2Config. Para obter mais informações, consulte EC2Config e AWS Systems Manager (p. 534). Se você tiver um proxy configurado no EC2Config, precisará atualizar suas configurações de proxy para o SSM Agent antes de fazer o upgrade. Se você não atualizar as configurações do proxy, não poderá usar o comando Executar para gerenciar suas instâncias. Para evitar isso, consulte as informações a seguir antes de atualizar a versão mais nova: Installing and Configuring SSM Agent on Windows Instances (Instalar e configurar o SSM Agent nas instâncias do Windows) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager). Se você tiver previamente habilitado a integração com o CloudWatch nas suas instâncias usando um arquivo de configuração local (<code>AWS.EC2.Windows.CloudWatch.json</code>), precisará configurar o arquivo para trabalhar com o SSM Agent. 	
3.19.1153	<ul style="list-style-type: none"> Reativado o plug-in de ativação para instâncias com a configuração antiga do AWS KMS. Altere o comportamento padrão do TRIM para estar desabilitado durante a operação de formatação do disco e adicione <code>FormatWithTRIM</code> para sobrescrever o plug-in <code>InitializeDisks</code> com <code>userdata</code>. 	
3.18.1118	<ul style="list-style-type: none"> Correção para adicionar rotas com confiança ao adaptador de rede primário. Atualizações para melhorar o suporte aos serviços da AWS. 	
3.17.1032	<ul style="list-style-type: none"> As correções duplicam os logs do sistema que aparecem quando os filtros são colocados na mesma categoria. Correções para evitar suspensão durante a inicialização do disco. 	
3.16.930	Adicionado suporte ao evento no log "A janela está pronta para usar" ao log do evento no Windows na inicialização.	
3.15.880	Correção para permitir upload da saída do Systems Manager Run Command para nomes do bucket S3 com o caractere ":".	
3.14.786	<p>Adicionado suporte para sobreescrivendo as configurações de plugin de <code>InitializeDisks</code>. Por exemplo: Para acelerar a inicialização do disco SSD, você pode temporariamente desabilitar o TRIM ao especificar o seguinte em <code>userdata</code>:</p> <pre><InitializeDrivesSettings><SettingsGroup>FormatWithoutTRIM</SettingsGroup></InitializeDrivesSettings></pre>	
3.13.727	Systems Manager Run Command – Correções dos comandos do processo com confiança após reinicialização do Windows.	

Versão	Detalhes	Data de lançamento
3.12.649	<ul style="list-style-type: none"> Correção para lidar tranquilamente com a reinicialização ao executar comandos/scripts. Correção para cancelar com confiança os comandos de execução. Adicione suporte para carregar (opcionalmente) logs de MSI no S3 ao instalar aplicações via Systems Manager Run Command. 	
3.11.521	<ul style="list-style-type: none"> Correções para permitir a geração de thumbprint de RDP para Windows Server 2003. Correções para incluir o fuso horário e a compensação do UTC nas linhas de log do EC2Config. Suporte a Systems Manager para executar comandos do Run Command em paralelo. Retornar à alteração anterior para colocar discos particionados online. 	
3.10.442	<ul style="list-style-type: none"> Corrigir falhas de configuração do Systems Manager ao instalar aplicações MSI. Correção para colocar discos de armazenamento online com confiança. Atualizações para melhorar o suporte aos serviços da AWS. 	
3.9.359	<ul style="list-style-type: none"> Correção no script pós-Sysprep para deixar a configuração do Windows atualizar em um estado padrão. Correção do plug-in de geração de senha para melhorar a confiabilidade ao obter as configurações da política de senha do GPO. Restrição às permissões da pasta do log de EC2Config/SSM ao grupo Administradores local. Atualizações para melhorar o suporte aos serviços da AWS. 	
3.8.294	<ul style="list-style-type: none"> Corrigido um problema com o CloudWatch que impedia os logs de serem atualizados quando não estivessem na unidade primária. Melhorado o processo de inicialização de disco ao adicionar a lógica de repetição. Adicionada manipulação de erro melhorada quando o plugin SetPassword falhava ocasionalmente durante a criação de AMI. Atualizações para melhorar o suporte aos serviços da AWS. 	
3.7.308	<ul style="list-style-type: none"> Melhorias ao utilitário ec2config-cli para testes de config e a solução de problemas dentro da instância. Evite adicionar rotas estáticas ao serviço de metadados do AWS KMS em um adaptador OpenVPN. Corrigido um problema no qual a execução de dados do usuário não estava honrando a tag "persist". A manipulação de erro melhorada ao fazer login no console do EC2 não está disponível. Atualizações para melhorar o suporte aos serviços da AWS. 	

Versão	Detalhes	Data de lançamento
3.6.269	<ul style="list-style-type: none"> Correção de confiabilidade da ativação do Windows para usar primeiro o endereço local do link 169.254.0.250/251 para ativar o Windows via AWS KMS Manuseio do proxy aprimorado para cenários de Systems Manager, Windows Activation e Domain Join Corrigido um problema em que linhas duplicadas de contas de usuário eram adicionadas ao arquivo de resposta do Sysprep 	
3.5.228	<ul style="list-style-type: none"> Resolvido um cenário em que o plugin do CloudWatch poderia consumir em excesso CPU e memória ao ler os logs de evento do Windows Adicionado um link para a documentação de configuração do CloudWatch na UI de configurações do EC2Config 	
3.4.212	<ul style="list-style-type: none"> Correções do EC2Config quando usadas em combinação com o VM Import. Corrigido o problema de nomeação do serviço no instalador do WiX. 	
3.3.174	<ul style="list-style-type: none"> Melhorada a manipulação de exceção para Systems Manager e falhas de junção de domínio. Alteração para dar suporte ao versionamento do esquema do Systems Manager SSM. Corrigida a formação de discos temporários em Win2K3. Alteração para suporte do tamanho do disco de configuração maior que 2TB. Uso reduzido de memória virtual ao definir o modo GC para padrão. Suporte para baixar artefatos do caminho UNC nos plugins <code>aws:psModule</code> e <code>aws:application</code>. Melhora no registro em log do plugin de ativação do Windows. 	
3.2.97	<ul style="list-style-type: none"> Melhorias de performance ao atrasar o carregamento de montagens do Systems Manager SSM. Melhora na manipulação de exceção para <code>sysprep2008.xml</code> malformado. Suporte à linha de comando para a configuração "Apply (Aplicar)" do Systems Manager. Alteração para suporte de união do domínio quando houver uma renomeação de computador pendente. Suporte para parâmetros opcionais no plugin <code>aws:applications</code>. Suporte para o array de comando no plugin <code>aws:psModule</code>. 	

Versão	Detalhes	Data de lançamento
3.0.54	<ul style="list-style-type: none"> Habilitar suporte para Systems Manager. O domínio integra automaticamente as instâncias do EC2 do Windows a um diretório da AWS via Systems Manager. Configure e carregue logs/métricas do CloudWatch via Systems Manager. Instale os módulos do PowerShell via Systems Manager. Instale as aplicações de MSI via Systems Manager. 	
2.4.233	<ul style="list-style-type: none"> Adicionada uma tarefa programada para recuperar o EC2Config de falhas o startup do serviço. Melhorias nas mensagens de erro do log do Console. Atualizações para melhorar o suporte aos serviços da AWS. 	
2.3.313	<ul style="list-style-type: none"> Corrigido o problema do grande consumo de memória em alguns casos quando o recurso CloudWatch Logs estiver habilitado. Corrigido um bug no upgrade, de forma que versões do EC2Config anteriores à 2.1.19 agora podem atualizar para a mais recente. Atualizada a exceção de abertura de porta COM para ser mais amigável e útil em logs. A UI do Ec2configServiceSettings desabilitou o redimensionamento e corrigiu a atribuição e o posicionamento de exibição da versão na UI. 	
2.2.12	<ul style="list-style-type: none"> NullPointerException processado ao consultar uma chave do registro para determinar o estado do Windows Sysprep que retorna nulo ocasionalmente. Liberados recursos não gerenciados no bloco final. 	
2.2.11	Corrigido um problema no plug-in do CloudWatch para lidar com linhas vazias do log.	
2.2.10	<ul style="list-style-type: none"> Removidas a configuração dos ajustes dos CloudWatch Logs por meio de UI. Permitir que os usuários definam configurações do CloudWatch Logs no arquivo %ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json para permitir melhorias futuras. 	
2.2.9	Corrigida a exceção não gerenciada e adicionado registro em log.	
2.2.8	<ul style="list-style-type: none"> Corrigir verificação da versão do SO do Windows no instalador do EC2Config para dar suporte ao Windows Server 2003 SP1 e posterior. Corrigir o manuseio do valor nulo ao ler as chaves de registro relacionadas à atualização dos arquivos de config do Sysprep. 	
2.2.7	<ul style="list-style-type: none"> Adicionado suporte para o EC2Config executar durante a execução do Sysprep para Windows 2008 e posterior. Manipulação de exceções aperfeiçoada e registro em log para melhores diagnósticos 	

Versão	Detalhes	Data de lançamento
2.2.6	<ul style="list-style-type: none"> • Reduzida a carga na instância e no CloudWatch Logs ao carregar os eventos de log. • Resolvido um problema de upgrade, no qual o plug-in do CloudWatch Logs nem sempre ficava habilitado 	
2.2.5	<ul style="list-style-type: none"> • Adicionado suporte ao carregamento de logs para o CloudWatch Log Service. • Corrigido um problema de condição de raça no plug-in Ec2OutputRDPCert • Alterada a opção de recuperação do serviço EC2Config para reiniciar a partir de TakeNoAction • Adicionada mais informações de exceção quando o EC2Config dá erro 	
2.2.4	<ul style="list-style-type: none"> • Corrigido um erro em PostSysprep.cmd • Corrigido o bug em que o EC2Config não se fixa no menu Iniciar para OS2012+ 	
2.2.3	<ul style="list-style-type: none"> • Adicionada opção de instalar o EC2Config sem que o serviço comece imediatamente após a instalação. Para usar, execute 'Ec2Install.exe start=false' pelo prompt de comando • Adicionado parâmetro no plug-in do papel de parede para controlar a adição/remoção do papel de parede. Para usar, execute "Ec2WallpaperInfo.exe set" ou "Ec2WallpaperInfo.exe revert" no prompt de comando • Adicionada verificação da chave RealTimelUniversal, configurações incorretas de saída da chave de registro de RealTimelUniversal para o console • Removida dependência do EC2Config na pasta de temporários do Windows • Removida dependência de execução de UserData no .Net 3.5 	
2.2.2	<ul style="list-style-type: none"> • Adicionada a verificação para comportamento de parada de serviço para verificar se os recursos estão sendo liberados • Corrigido o problema com longos períodos de execução ao ingressar no domínio 	
2.2.1	<ul style="list-style-type: none"> • Atualizado o instalador para permitir upgrades de versões mais antigas • Corrigido o bug Ec2WallpaperInfo no ambiente exclusivo do .Net4.5 • Corrigindo o bug de detecção do driver intermitente • Adicionada a opção de instalação silenciosa. Execute Ec2Install.exe com a opção '-q', por exemplo: 'Ec2Install.exe -q' 	
2.2.0	<ul style="list-style-type: none"> • Adicionado suporte para ambientes exclusivos de .Net4 e .Net4.5 • Atualizado o instalador 	

Versão	Detalhes	Data de lançamento
2.1.19	<ul style="list-style-type: none"> • Adicionado suporte à etiqueta do disco efêmera ao usar o driver de rede da Intel (por exemplo, tipo de instância C3). Para obter mais informações, consulte Rede avançada no Windows (p. 1028). • Adicionado suporte à versão de origem da AMI e ao nome de origem da AMI para a saída do console • Alterações feitas à saída do Console para formatação/análise consistente • Arquivo de ajuda atualizado 	
2.1.18	<ul style="list-style-type: none"> • Adicionado objetivo de WMI do EC2Config para notificação de conclusão (-Namespace root\Amazon -Class EC2_ConfigService) • Performance aprimorada da consulta de WMI de startup com grandes logs de evento; pode causar uso elevado prolongado da CPU durante a execução inicial 	
2.1.17	<ul style="list-style-type: none"> • Corrigido problema de execução com enchimento de buffer de saída padrão e erro padrão • O thumbprint de RDP incorreto fixo que às vezes aparece em saída do console para o SO >= w2k8 • A saída do console agora contém "RDPCERTIFICATE-SubjectName:" para Windows 2008+, que contém o valor do nome da máquina • Adicionado D:\ ao menu suspenso de mapeamento da letra de unidade • Movido o botão Ajuda para o canto direito superior e alterada a aparência • Adicionado link de pesquisa de Feedback ao canto direito superior 	
2.1.16	<ul style="list-style-type: none"> • A guia Geral inclui o link da página de download do EC2Config para novas versões • A sobreposição do papel de parede do desktop agora está armazenada na pasta Users Local Appdata, em vez de em Meus Documentos, compatível com o redirecionamento do MyDoc • Nome do MSSQLServer sincronizado com o sistema no script do Post-Sysprep (2008+) • Pasta de aplicação reordenada (arquivos movidos para o diretório Plugin e removidos os arquivos em duplicata) • Alterada saída do log do sistema (Console): <ul style="list-style-type: none"> • *Movido para o formato data, nome, valor para facilitar a análise (comece a migrar as dependências para um novo formato) • *Adicionado o status do plugin 'Ec2SetPassword' • *Adicionado a hora de início e fim do Sysprep • Corrigido o problema de discos temporários não serem marcados como "Armazenamento Temporário" para sistemas operacionais não em inglês • Corrigida a falha de desinstalação do EC2Config depois de executar Sysprep 	

Versão	Detalhes	Data de lançamento
2.1.15	<ul style="list-style-type: none"> Solicitações otimizadas do serviço de metadados Os metadados agora contornam as configurações do proxy Discos temporários marcados como "Armazenamento temporário" e Important.txt colocados no volume quando encontrados (somente drivers do Citrix PV). Para obter mais informações, consulte Atualizar drivers de PV em instâncias do Windows (p. 565). Discos temporários com letras Z a A (somente drivers do Citrix PV) – a atribuição pode ser sobreescrita usando o plug-in de mapeamento de letra da unidade com etiquetas de Volume "Armazenamento Temporário X", onde x é um número 0-25 O UserData agora é executado imediatamente depois de "Windows está pronto" 	
2.1.14	Correções do papel de parede do desktop	
2.1.13	<ul style="list-style-type: none"> Por padrão, o papel de parede do desktop exibirá o hostname Dependência removida do serviço de Horário do Windows Rota adicionada nos casos em que vários IPs são atribuídos a uma única interface 	
2.1.11	<ul style="list-style-type: none"> Alterações feitas no plug-in Ec2Activation - Verifica o status de Ativação cada 30 dias - Se o período de carência tiver 90 dias restantes (dos 180), tenta novamente a ativação 	
2.1.10	<ul style="list-style-type: none"> A sobreposição do papel de parede do desktop não persiste mais com Sysprep ou desativação sem Sysprep Opção de UserData para executar em cada início de serviço com <persist>true</persist> Local e nome alterados de /DisableWinUpdate.cmd para /Scripts/PostSysprep.cmd Senha do administrador definida para não expirar por padrão em / Scripts/PostSysprep.cmd A desinstalação removerá o script PostSysprep do EC2Config c:\windows\setup\script\CommandComplete.cmd O Add Route suporta métricas de interface personalizada 	
2.1.9	A execução de UserData não é mais limitada a 3851 caracteres	

Versão	Detalhes	Data de Lançamento
2.1.7	<ul style="list-style-type: none"> • Identificador da versão do SO e do idioma gravado no console • Versão do EC2Config gravada no console • Versão do driver PV gravada no console • Detecção de verificação de bugs e saída para o console na inicialização seguinte, quando encontrado • Adicionada opção para o config.xml manter as credenciais de Sysprep • Adicionar lógica de Route Retry nos casos em que o ENI está indisponível na inicialização • PID de execução dos dados do usuário gravados no console • Comprimento mínimo de senha gerado recuperado de GPO • Ajuste o início do serviço para refazer 3 tentativas • Adicionados exemplos S3_DownloadFile.ps1 e S3_Upload file.ps1 à pasta /Scripts 	
2.1.6	<ul style="list-style-type: none"> • Informações da versão adicionadas à guia Geral • Guia Pacote renomeada para Imagem • Simplificado o processo de especificação de senhas e movidas as UIs relacionadas à senha da guia Geral para a guia Imagem • Guia Configurações do disco rebatizada de Armazenamento • Adicionada a guia Suporte com ferramentas comuns para a resolução de problemas • sysprep.ini do Windows 2003 configurado para ampliar a partição do SO por padrão • Adicionado o endereço IP privado ao papel de parede • Endereço IP privado exibido no papel de parede • Lógica de tentativas adicionada à saída do Console • Exceção da porta de Com fixa para acessibilidade de metadados – fez com que o EC2Config fosse encerrado, pois a saída do console é exibida • Verifica o status da ativação em cada inicialização – ativa conforme o necessário • Problema corrigido de caminhos relativos – causado ao executar manualmente o atalho do papel de parede pela pasta de startup; apontando para Administrador/logs • Cor de fundo padrão corrigida para usuário do Windows Server 2003 (além do Administrador) 	

Versão	Detalhes	Data de lançamento
2.1.2	<ul style="list-style-type: none"> • Timestamps do console em UTC (Zulu) • Removida a aparência hyperlink na guia Sysprep • Adição de recurso para expandir dinamicamente o volume do dispositivo raiz na primeira inicialização para Windows 2008+ • Quando a opção Set-Password estiver habilitada, permite automaticamente que o EC2Config defina a senha • O EC2Config verifica o status de ativação antes de executar o Sysprep (apresenta uma advertência se não estiver ativado) • O <code>Sysprep.xml</code> do Windows Server 2003 agora usa como padrão o fuso horário UTC em vez de hora do Pacífico • Servidores de ativação aleatórios • Guia Mapeamento da unidade rebatizada para Configurações do disco • Itens de UI de Inicializar unidades movidas da guia Geral para a guia Configurações do disco • O botão Ajuda agora aponta para o arquivo de ajuda HTML • Arquivo HTML de ajuda atualizado com alterações • Texto "Observação" atualizado para mapeamentos das letras da unidade • Adicionado <code>InstallUpdates.ps1</code> à pasta <code>/Scripts</code> para automatizar patches e limpeza antes de Sysprep 	
2.1.0	<ul style="list-style-type: none"> • O papel de parede do desktop exibe informações da instância por padrão no primeiro logon (não desconectar/reconectar) • O PowerShell pode ser executado a partir de userdata ao cercar o código com <code><powershell></powershell></code> 	

Assinar as notificações de serviço do EC2Config

O Amazon SNS pode notificá-lo quando novas versões do serviço EC2Config forem liberadas. Use o procedimento a seguir para se inscrever nessas notificações.

Para se inscrever nas notificações do EC2Config

1. Abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. Você deve selecionar esta Região porque as notificações do SNS que você está assinando foram criadas nesta Região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
 - a. Para o ARN do tópico, use o seguinte ARN (nome de recurso da Amazon):

`arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config`

 - b. Para Protocolo, selecione Email.
 - c. Para Endpoint, digite um endereço de e-mail que você pode usar para receber as notificações.
 - d. Selecione Create subscription.

6. Você receberá um e-mail solicitando que você confirme sua assinatura. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que uma nova versão do serviço EC2Config for liberada, nós enviaremos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a inscrição das notificações do EC2Config

1. Abra o console do Amazon SNS.
2. No painel de navegação, escolha Subscriptions.
3. Selecione a assinatura e escolha Actions, Delete subscriptions. Quando solicitado para confirmação, escolha Delete.

Solucionar problemas com o serviço do EC2Config

As informações a seguir podem ajudá-lo a resolver problemas com o serviço EC2Config.

Atualizar o EC2Config em uma instância inacessível

Use o procedimento a seguir para atualizar o serviço EC2Config em uma instância do Windows Server inacessível usando o Desktop Remoto.

Para atualizar o EC2Config em um a instância do Windows baseada em Amazon EBS à qual você não pode se conectar

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize a instância afetada. Selecione a instância e escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância).

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Escolha Launch instances (Executar instância) e crie uma instância t2.micro temporária na mesma zona de disponibilidade que a instância afetada. Use uma AMI diferente da que você usou para executar a instância afetada.

Important

Se você não criar a instância na mesma zona de disponibilidade que a instância afetada, não conseguirá associar o volume do dispositivo raiz da instância afetada à nova instância.

5. No console do EC2, selecione Volumes.
6. Localize o volume do dispositivo raiz da instância afetada. [Desanexe o volume \(p. 1290\)](#) e [anexe o volume \(p. 1271\)](#) à instância temporária criada anteriormente. Associe-a com o nome do padrão do dispositivo (xvdf).
7. Use o Desktop Remoto para conectar-se à instância temporária e use em utilitário Gerenciamento de Disco para [disponibilizar o volume para uso \(p. 1272\)](#).
8. [Faça download](#) da versão mais recente do serviço EC2Config. Extraia arquivos do arquivo .zip para o diretório Temp na unidade que você associou.
9. Na instância temporária, abra a caixa de diálogo Run (Executar), digite **regedit** e pressione Enter.

10. Escolha `HKEY_LOCAL_MACHINE`. No menu Arquivo, escolha Carregar Hive. Escolha a unidade, vá até ele e abra o seguinte arquivo: `Windows\System32\config\SOFTWARE`. Quando solicitado, especifique o nome da chave.
11. Selecione a chave que você acabou de carregar e vá até `Microsoft\Windows\CurrentVersion`. Escolha a chave `RunOnce`. Se essa chave não existir, escolha `CurrentVersion` no menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Chave. Nomeie a chave `RunOnce`.
12. No menu contextual (clique com o botão direito do mouse), escolha a chave `RunOnce`, escolha Novo e escolha no Valor da string. Insira `Ec2Install` como o nome e `C:\Temp\Ec2Install.exe /quiet` como dados.
13. Escolha a chave `HKEY_LOCAL_MACHINE\specified key name\Microsoft\Windows NT\CurrentVersion\Winlogon`. No menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Valor da string. Insira `AutoAdminLogon` como o nome e `1` como dados.
14. Escolha a chave `HKEY_LOCAL_MACHINE\specified key name\Microsoft\Windows NT\CurrentVersion\Winlogon>`. No menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Valor da string. Insira `DefaultUserName` como o nome e `Administrator` como dados.
15. Escolha a chave `HKEY_LOCAL_MACHINE\specified key name\Microsoft\Windows NT\CurrentVersion\Winlogon`. No menu contextual (clique com o botão direito do mouse), escolha Novo e selecione Valor da string. Digite `DefaultPassword` como nome e digite uma senha nos dados de valor.
16. No painel de navegação do Editor de Registro, escolha a chave temporária que você criou quando abriu pela primeira vez o Editor de Registro.
17. No menu Arquivo, escolha Descarregar Hive.
18. No utilitário Gerenciamento de Disco, escolha o disco que você anexou anteriormente, abra o menu de contexto (botão direito do mouse) e escolha Offline.
19. No console do Amazon EC2, separe o volume afetado da instância temporária e reanexe-o à instância original com o nome de dispositivo `/dev/sda1`. Você deve especificar o nome desse dispositivo para designar o volume como volume do dispositivo raiz.
20. [Interromper e iniciar sua instância \(p. 455\)](#) a instância.
21. Depois que a instância for iniciada, verifique o log do sistema e veja se a mensagem Windows is ready to use aparece.
22. Abra o Editor de Registro e escolha `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. Exclua as chaves de valor da string criada anteriormente: `AutoAdminLogon`, `DefaultUserName` e `DefaultPassword`.
23. Exclua ou interrompa a instância temporária que você criou nesse procedimento.

Drivers paravirtuais para as instâncias do Windows

As AMIs do Windows contêm um conjunto de drivers para permitir acesso ao hardware virtualizado. Esses drivers são usados pelo Amazon EC2 para mapear armazenamento de instâncias e volumes do Amazon EBS para seus dispositivos. A tabela a seguir mostra as principais diferenças entre os diferentes drivers.

	RedHat PV	Citrix PV	AWS PV
Tipo de instância	Não tem suporte para todos os tipos de instâncias. Se você especificar um tipo de instância sem suporte, a instância ficará danificada.	Com suporte para os tipos de instância Xen.	Com suporte para os tipos de instância Xen.

	RedHat PV	Citrix PV	AWS PV
Volumes anexados	Oferece suporte a até 16 volumes anexados.	Oferece suporte a mais de 16 volumes anexados.	Oferece suporte a mais de 16 volumes anexados.
Rede	O driver tem problemas conhecidos em que a conexão de rede é redefinida em cargas altas, por exemplo, transferências rápidas de arquivos via FTP.		O driver configura automaticamente quadros jumbo no adaptador da rede quando está em um tipo de instância compatível. Quando a instância está em um placement group de cluster (p. 1044) , isso oferece melhor performance de rede entre as instâncias no placement group de cluster.

A tabela a seguir mostra quais drivers PV você deve executar em cada versão do Windows Server no Amazon EC2.

Versão Windows Server	Versão PV driver
Windows Server 2019	AWSVersão mais recente do PV
Windows Server 2016	AWSVersão mais recente do PV
Windows Server 2012 R2	AWSVersão mais recente do PV
Windows Server 2012	AWSVersão mais recente do PV
Windows Server 2008 R2	AWS PV versão 8.3.4 e anterior
Windows Server 2008	Citrix PV 5.9
Windows Server 2003	Citrix PV 5.9

Tópicos

- [AWSDrivers PV \(p. 561\)](#)
- [Drivers do Citrix PV \(p. 564\)](#)
- [Drivers RedHat PV \(p. 564\)](#)

- Assinar notificações do (p. 565)
- Atualizar drivers de PV em instâncias do Windows (p. 565)
- Solucionar problemas de drivers de PV (p. 571)

AWSDrivers PV

Os drivers AWS PV são armazenadas no diretório %ProgramFiles%\Amazon\Xentools. Esse diretório também contém símbolos públicos e uma ferramenta de linha de comando, `xenstore_client.exe`, que permite acessar entradas no XenStore. Por exemplo, o seguinte comando de PowerShell retorna o horário atual do Hypervisor:

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

Os componentes do driver AWS PV são listados no Registro do Windows em `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`. Esses componentes do driver são os seguintes: `xenbus`, `xeniface`, `xennet`, `xenvbd` e `xenvif`.

AWSOs drivers PV também têm um serviço do Windows chamado LiteAgent, que é executado no modo de usuário. Ele lida com tarefas como eventos de desligamento e reinicialização a partir das APIs da AWS em instâncias de geração Xen. Você pode acessar e gerenciar serviços executando `Services.msc` a partir da linha de comando. Quando executados em instâncias de geração Nitro, os drivers AWS PV não são usados e o serviço LiteAgent será interrompido automaticamente começando pela versão do driver 8.2.4. A atualização para o driver AWS PV mais recente também atualiza o LiteAgent e melhora a confiabilidade em todas as gerações de instâncias.

Instalar os drivers AWS PV mais recentes

As AMIs Windows da Amazon contêm um conjunto de drivers para permitir acesso ao hardware virtualizado. Esses drivers são usados pelo Amazon EC2 para mapear armazenamento de instâncias e volumes do Amazon EBS para seus dispositivos. Recomendamos que você instale os drivers mais recentes para melhorar a estabilidade e a performance de suas instâncias do EC2 Windows.

Opções de instalação

- Você pode usar o AWS Systems Manager automaticamente para atualizar os drivers PV. Para obter mais informações, consulte [Walkthrough: Automatically Update PV Drivers on EC2 Windows Instances \(Console\) \(Demonstração: atualizar automaticamente drivers PV em instâncias Windows do EC2 \(console\)\)](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).
- Você pode fazer [download](#) do pacote de configuração do driver e executar o programa de instalação manualmente. Verifique o arquivo `readme.txt` quanto aos requisitos do sistema. Para obter informações sobre como fazer download e instalar os drivers AWS PV ou se você estiver atualizando um controlador de domínio, consulte [Atualizar instâncias do Windows Server \(atualização do AWS PV\) \(p. 566\)](#).

AWSHistórico do pacote de drivers PV

A tabela a seguir mostra as alterações nos drivers AWS PV para cada versão de driver.

Versão do pacote	Detalhes	Data de lançamento
8.4.0	<ul style="list-style-type: none">Correções de estabilidade para resolver casos raros de E/S de disco preso.	2 de março de 2021

Versão do pacote	Detalhes	Data de lançamento
	<ul style="list-style-type: none"> Correções de estabilidade para resolver casos raros de falhas durante a desanexação do volume EBS. Recurso adicionado para distribuir carga em vários núcleos para workloads que usam mais de 20.000 IOPS e experimentam degradação devido a gargalos. Para ativar esse recurso, consulte Workloads que usam mais de 20.000 IOPS de disco apresentam degradação devido a gargalos da CPU (p. 577). A instalação do AWS PV 8.4 no Windows Server 2008 R2 falhará. AWS O PV versão 8.3.4 e versões anteriores são compatíveis com o Windows Server 2008 R2. 	
8.3.4	Maior confiabilidade do anexo do dispositivo de rede.	4 de agosto de 2020
8.3.3	<ul style="list-style-type: none"> Atualize para o componente voltado para o XenStore a fim de evitar a verificação de bugs durante os caminhos de manipulação de erros. Atualize para o componente de armazenamento para evitar falhas quando um SRB inválido for enviado. <p>Para atualizar esse driver em instâncias do Windows Server 2008 R2, você deve primeiro verificar se os patches apropriados estão instalados para abordar o seguinte Aviso de segurança da Microsoft: Aviso de segurança da Microsoft 3033929.</p>	4 de fevereiro de 2020
8.3.2	Confiabilidade aprimorada de componentes da rede.	30 de julho de 2019
8.3.1	Melhora na performance e na robustez do componente de armazenamento.	12 de junho de 2019
8.2.7	Maior eficiência para oferecer suporte à migração para os tipos de instância de última geração.	20 de maio de 2019
8.2.6	Eficiência aumentada do caminho de despejo de memória.	15 de janeiro de 2019
8.2.5	Melhorias de segurança adicionais. O instalador do PowerShell agora está disponível no pacote.	12 de dezembro de 2018
8.2.4	Melhorias na confiabilidade.	2 de outubro de 2018
8.2.3	Correções de erros e melhorias na performance. Relate o ID de volume do EBS como o número de série do disco para volumes do EBS. Isso permite cenários de cluster, como o S2D.	29 de maio de 2018
8.2.1	Melhorias de performance de rede e de armazenamento e várias correções de solidez. Para verificar se esta versão foi instalada, consulte o valor do seguinte registro do Windows: <code>HKEY_LOCAL_MACHINE\Software\Amazon\PVDriver\Version</code> 8.2.1.	8 de março de 2018

Versão do pacote	Detalhes	Data de lançamento
7.4.6	Correções de estabilidade para tornar os drivers AWS PV mais resilientes.	26 de abril de 2017
7.4.3	Adicionado suporte para o Windows Server 2016. Correções de estabilidade para todas as versões dos sistemas operacionais Windows com suporte. *AWSA assinatura da versão 7.4.3 do driver PV expira em 29 de março de 2019. Recomendamos que você atualize para o driver AWS PV mais recente.	18 de nov de 2016
7.4.2	Correções de estabilidade para suporte do tipo de instância X1.	2 de agosto de 2016
7.4.1	<ul style="list-style-type: none"> • Melhoria da performance no driver AWS PV Storage. • Correções de estabilidade no driver AWS PV Storage: corrigido um problema em que as instâncias sofriam uma paralisação do sistema com o código de verificação de bugs 0x0000DEAD. • Correções de estabilidade no driver AWS PV Network. • Adicionado suporte para o Windows Server 2008R2. 	12 de julho de 2016
7.3.2	<ul style="list-style-type: none"> • Aperfeiçoados o registro em log e o diagnóstico. • Correção de estabilidade no driver AWS PV Storage. Em alguns casos, os discos podem não ser expostos no Windows depois de anexar novamente o disco à instância. • Adicionado suporte para o Windows Server 2012. 	24 de junho de 2015
7.3.1	Atualização TRIM: correção relativa às solicitações TRIM. Essa correção estabiliza as instâncias e melhora a performance da instância ao gerenciar um grande número de solicitações TRIM.	
7.3.0	Suporte TRIM: o driver AWS PV agora envia solicitações TRIM para o hipervisor. Os discos efêmeros processarão adequadamente as solicitações TRIM desde que o armazenamento subjacente ofereça suporte a TRIM (SSD). Observe que o armazenamento baseado em EBS não oferece suporte a TRIM desde março de 2015.	
7.2.5	<ul style="list-style-type: none"> • Correção de estabilidade em drivers AWS PV Storage: em alguns casos, o driver AWS PV pode cancelar a referência de memória inválida e causar uma falha de sistema. • Correção de estabilidade ao gerar um despejo de memória: em alguns casos o driver AWS PV trava em um condição de disputa ao gravar um despejo de memória. Antes dessa versão, só era possível resolver o problema forçando o driver a interromper e reiniciar, o que fazia com que o despejo de memória fosse perdido. 	
7.2.4	Manutenção do ID de dispositivo: essa correção de driver mascara o ID do dispositivo PCI da plataforma e força o sistema a sempre expor o mesmo ID de dispositivo, mesmo que a instância seja movida. De uma forma mais geral, a correção afeta como o hipervisor expõe dispositivos virtuais. A correção também inclui modificações ao instalador dos drivers AWS PV de forma que o sistema mantenha dispositivos virtuais mapeados.	

Versão do pacote	Detalhes	Data de lançamento
7.2.2	<ul style="list-style-type: none"> Carga dos drivers AWS PV no modo Directory Services Restore Mode (DSRM): o modo Directory Services Restore é uma opção de inicialização do modo de segurança para controladores de domínio do Windows Server. Manutenção do ID do dispositivo quando o dispositivo de adaptador de rede virtual é anexado novamente: essa correção força o sistema a verificar o mapeamento de endereço MAC e a manter o ID do dispositivo. Essa correção garante que os adaptadores retenham suas configurações estáticas se os adaptadores forem anexados novamente. 	
7.2.1	<ul style="list-style-type: none"> Execução no modo de segurança: corrigido o problema em que o driver não era carregado no modo de segurança. Anteriormente, os drivers AWS PV só instanciavam em sistemas de execução normal. Adição de discos aos grupos de armazenamento do Microsoft Windows: anteriormente, sintetizávamos as consultas da página 83. A correção desabilitou o suporte da página 83. Isso não afeta os grupos de armazenamento que são usados em um ambiente de cluster porque os discos PV não são discos de cluster válidos. 	
7.2.0	Base: A versão base do AWS PV.	

Drivers do Citrix PV

Os drivers Citrix PV são armazenados no diretório %ProgramFiles%\Citrix\XenTools (instâncias de 32 bits) ou %ProgramFiles(x86)%\Citrix\XenTools (instâncias de 64 bits).

Os componentes do driver Citrix PV são listados no Registro do Windows em HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services. Esses componentes de driver são os seguintes: xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd e xenvif.

O Citrix também tem um componente de driver chamado XenGuestAgent, que é executado como um serviço do Windows. Ele lida com tarefas como eventos de desligamento e reinicialização a partir da API. Você pode acessar e gerenciar serviços executando Services.msc a partir da linha de comando.

Se você estiver encontrando erros de redes ao executar determinadas workloads, precisará desabilitar o recurso de descarregamento de TCP para o driver Citrix PV. Para obter mais informações, consulte [Descarregamento de TCP \(p. 576\)](#).

Drivers RedHat PV

Os drivers RedHat têm suporte para instâncias herdadas, mas não são recomendados em instâncias mais novas com mais de 12 GB de RAM devido às limitações do driver. As instâncias com mais de 12 GB de RAM que executam drivers RedHat podem não ser iniciadas e se tornar inacessíveis. Recomendamos atualizar os drivers RedHat para drivers Citrix PV e, em seguida, atualizar os drivers Citrix PV para drivers AWS PV.

Os arquivos de origem para os drivers RedHat estão no diretório %ProgramFiles%\RedHat (instâncias de 32 bits) ou %ProgramFiles(x86)%\RedHat (instâncias de 64 bits). Os dois drivers são rhelnet, o driver de rede paravirtualizado RedHat e rhelscsi, o driver miniporta SCSI RedHat.

Assinar notificações do

O Amazon SNS pode notificá-lo quando novas versões dos drivers EC2 para Windows são lançadas. Use o procedimento a seguir para se inscrever nessas notificações.

Como assinar as notificações do EC2 no console

1. Abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região porque as notificações do SNS que você está assinando estão nesta região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
 - a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):
`arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers`
 - b. Para Protocolo, selecione Email.
 - c. Para Endpoint, digite um endereço de e-mail que você pode usar para receber as notificações.
 - d. Selecione Create subscription.
6. Você receberá um e-mail de confirmação. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que novos drivers EC2 para Windows são lançados, nós enviamos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações do driver Amazon EC2 para Windows

1. Abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.
2. No painel de navegação, escolha Subscriptions.
3. Marque a caixa de seleção da assinatura e, depois, selecione Actions (Ações), Delete subscriptions (Excluir assinaturas). Quando a confirmação for solicitada, escolha Excluir.

Para assinar as notificações do EC2 usando a AWS CLI

Para assinar as notificações do EC2 com a AWS CLI, use o comando a seguir.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --  
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Para assinar as notificações do EC2 usando a AWS Tools for PowerShell

Para assinar as notificações do EC2 com Tools for Windows PowerShell, use o comando a seguir.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers'  
-Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Atualizar drivers de PV em instâncias do Windows

Recomendamos que você instale os drivers de PV mais recentes para melhorar a estabilidade e a performance de suas instâncias do EC2 Windows. As instruções desta página ajudam você a fazer download do pacote do driver e executar o programa de instalação.

Para verificar qual driver sua instância do Windows usa

Abra Network Connections (Conexões de rede) no Painel de controle e consulte Conexão de área local. Verifique se o driver é um dos seguintes:

- AWS PV Network Device
- Citrix PV Ethernet Adapter
- Driver RedHat PV NIC

Como alternativa, você pode verificar a saída do comando `pnputil -e`.

Requisitos do sistema

Verifique o arquivo `readme.txt` no download quanto aos requisitos do sistema.

Tópicos

- [Atualizar instâncias do Windows Server \(atualização do AWS PV\) \(p. 566\)](#)
- [Atualizar um controlador de domínio \(atualização do AWS PV\) \(p. 567\)](#)
- [Atualizar instâncias do Windows Server 2008 e 2008 R2 \(atualização do Redhat para Citrix PV\) \(p. 569\)](#)
- [Atualizar o serviço de agente convidado do Citrix Xen \(p. 571\)](#)

Atualizar instâncias do Windows Server (atualização do AWS PV)

Use o seguinte procedimento para executar uma atualização no local dos drivers AWS PV ou fazer uma atualização de drivers Citrix PV para drivers AWS PV no Windows Server 2008 R2, no Windows Server 2012, no Windows Server 2012 R2, no Windows Server 2016 ou no Windows Server 2019. Essa atualização não está disponível para drivers RedHat nem outras versões do Windows Server.

Important

Se sua instância for um controlador de domínio, consulte [Atualizar um controlador de domínio \(atualização do AWS PV\) \(p. 567\)](#). O processo de atualização dessas instâncias do controlador de domínio é diferente das edições padrão do Windows.

Atualizar drivers AWS PV

1. Recomendamos que você crie uma AMI como backup da seguinte forma, caso precise reverter suas alterações.
 - a. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.
 - b. No painel de navegação, escolha Instances (Instâncias).
 - c. Selecione a instância que requer a atualização do driver e escolha Instance state (Estado da instância), Stop Instance (Parar instância).
 - d. Depois que a instância for interrompida, selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).
 - e. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).
2. Conectar-se à instância usando o Desktop Remoto.
3. Recomendamos que você desative todos os discos que não sejam do sistema e anote quaisquer mapeamentos de letras de unidade para os discos secundários no Gerenciamento de Disco antes

de executar esta atualização. Essa etapa não será necessária se você executar uma atualização no local dos drivers AWS PV. Também recomendamos definir serviços não essenciais como inicialização Manual no console de Services.

4. [Faça download](#) do pacote de drivers mais recente na instância.

Ou execute o seguinte comando do PowerShell:

```
PS C:\> invoke-webrequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip  
expand-archive $env:UserProfile\pv_driver.zip -DestinationPath  
$env:UserProfile\pv_drivers
```

5. Extraia o conteúdo da pasta e execute AWSPVDriverSetup.msi.

Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza o driver. A instância não estará disponível por até 15 minutos. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, você poderá verificar se o novo driver foi instalado conectando-se à instância usando o Remote Desktop e executando o seguinte comando do PowerShell:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte [AWSHistórico do pacote de drivers PV \(p. 561\)](#). Abra o Gerenciamento de disco para revisar todos os volumes secundários offline e colocá-los online correspondendo às letras da unidade observadas na Etapa 6.

Se você desabilitou anteriormente o [Descarregamento de TCP \(p. 576\)](#) usando Netsh para drivers Citrix PV, recomendamos reabilitar esse recurso depois de fazer a atualização para drivers AWS PV. Os problemas de descarregamento de TCP com os drivers Citrix não estão presentes nos drivers AWS PV. Como resultado, o descarregamento de TCP proporciona um melhor performance com os drivers AWS PV.

Se você aplicou anteriormente um endereço IP estático ou a configuração de DNS À interface de rede, reaplique o endereço IP estático ou a configuração de DNS depois de atualizar os drivers AWS PV.

Atualizar um controlador de domínio (atualização do AWS PV)

Use o procedimento a seguir em um controlador de domínio para executar uma atualização no local dos drivers AWS PV ou atualizar drivers Citrix PV para drivers AWS PV.

Para atualizar um controlador de domínio

1. Recomendamos que você crie um backup do seu controlador de domínio no caso de precisar reverte suas alterações. O uso de uma AMI como backup não é suportado. Para obter mais informações, consulte [Considerações de backup e restauração para controladores de domínio virtualizados](#) na documentação da Microsoft.
2. Execute o comando a seguir para configurar o Windows para ser iniciado no Modo de Restauração dos Serviços de Diretório (DSRM):

Warning

Antes de executar esse comando, confirme a senha do DSRM. Você precisará dessas informações para fazer login na sua instância depois que a atualização estiver concluída e a instância tiver sido reiniciada automaticamente.

```
bcdedit /set {default} safeboot dsrepair
```

PowerShell:

```
PS C:\> bcdedit /set "{default}" safeboot dsrepair
```

O sistema deve ser inicializado no DSRM porque o utilitário de atualização remove os drivers de armazenamento Citrix PV para que possa instalar os drivers AWS PV. Por isso, recomendamos que anote quaisquer mapeamentos de letras e pastas de unidade para os discos secundários no Gerenciamento de Disco. Quando os drivers de armazenamento Citrix PV não estiverem presentes, as unidades secundárias não serão detectadas. Os controladores de domínio que usam uma pasta NTDS em unidades secundárias não serão inicializados porque o disco secundário não será detectado.

Warning

Depois de executar esse comando não reinicialize o sistema manualmente. O sistema ficará inacessível porque os drivers Citrix PV não oferecem suporte a DSRM.

3. Execute o comando a seguir para adicionar **DisableDCCheck** ao registro:

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t REG_SZ /d true
```

4. [Faça download](#) do pacote de drivers mais recente na instância.
5. Extraia o conteúdo da pasta e execute **AWSPVDriverSetup.msi**.

Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza o driver. A instância não estará disponível por até 15 minutos.

6. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop. Abra o Gerenciamento de disco para revisar todos os volumes secundários offline e colocá-los online correspondendo ao mapeamento de letras e pastas de unidade observado anteriormente.

Você deve se conectar à instância especificando o nome do usuário no seguinte formato `hostname\administrador`. Por exemplo, `Win2k12TestBox\administrador`.

7. Execute o comando a seguir para remover a configuração de inicialização do DSRM:

```
bcdedit /deletevalue safeboot
```

8. Reinicialize a instância.
9. Para concluir o processo de atualização, verifique se o novo driver foi instalado. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do AWS PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte [AWSHistórico do pacote de drivers PV \(p. 561\)](#).

10. Execute o comando a seguir para excluir **DisableDCCheck** do registro:

```
reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
```

Note

Se você desabilitou anteriormente o [Descarregamento de TCP \(p. 576\)](#) usando Netsh para drivers Citrix PV, recomendamos reabilitar esse recurso depois de fazer a atualização para drivers AWS PV. Os problemas de descarregamento de TCP com os drivers Citrix não estão presentes nos drivers AWS PV. Como resultado, o descarregamento de TCP proporciona um melhor performance com os drivers AWS PV.

Atualizar instâncias do Windows Server 2008 e 2008 R2 (atualização do Redhat para Citrix PV)

Antes você começar a atualizar seus drivers RedHat para drivers Citrix PV, faça o seguinte:

- Instale a versão mais recente do serviço EC2Config. Para obter mais informações, consulte [Instalar a versão mais recente do EC2Config \(p. 532\)](#).
- Verifique se você tem o Windows PowerShell 3.0 instalado. Para verificar a versão que você instalou, execute o seguinte comando em uma janela do PowerShell:

```
PS C:\> $PSVersionTable.PSVersion
```

O Windows PowerShell 3.0 está incluído no pacote de instalação do Windows Management Framework (WMF) versão 3.0. Se você precisar instalar o Windows PowerShell 3.0, consulte [Windows Management Framework 3.0](#) no Centro de Download da Microsoft.

- Faça backup de suas informações importantes sobre a instância ou crie uma AMI da instância. Para obter mais informações sobre a criação de uma AMI, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#). Se você criar uma AMI, certifique-se de fazer o seguinte:
 - Escreva sua senha.
 - Não execute a ferramenta Sysprep manualmente nem usando o serviço EC2Config.
 - Defina o adaptador de Ethernet para obter um endereço IP usando automaticamente o DHCP. Para obter mais informações, consulte [Definir as configurações de TCP/IP na Biblioteca do Microsoft TechNet](#).

Para atualizar drivers RedHat

1. Conecte-se à instância e faça login como administrador local. Para obter mais informações sobre como se conectar à sua instância, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
2. Em sua instância, [faça download](#) do pacote de atualização do Citrix PV.
3. Extraia o conteúdo dos pacotes de atualização para um local de sua escolha.
4. Clique duas vezes no arquivo Upgrade.bat. Se receber um aviso de segurança, selecione Executar.
5. Na caixa de diálogo Atualizar drivers, revise as informações e selecione Sim se você estiver pronto para iniciar a atualização.
6. Na caixa de diálogo Desinstalador dos drivers paravirtualizados Red Hat para Windows, selecione Sim para remover o software RedHat. Sua instância será recarregada.

Note

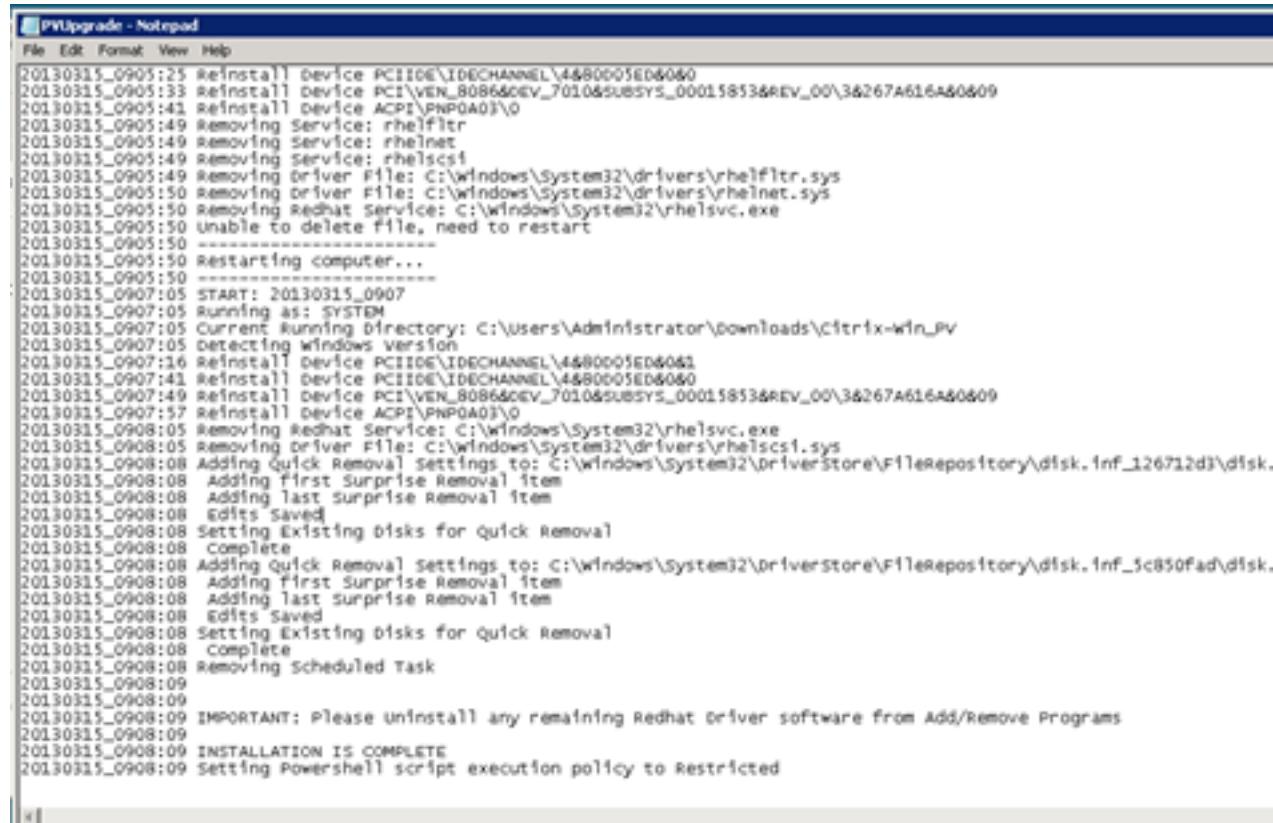
Se você não vir a caixa de diálogo do desinstalador, selecione Red Hat paravirtualizado na barra de tarefas do Windows.



7. Verifique se a instância foi reinicializada e está pronta para uso.
 - a. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
 - b. Na página Instances (Instâncias), selecione Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas) e, em seguida, escolha Get system log (Obter log do sistema).
 - c. As operações de atualização devem ter reiniciado o servidor 3 ou 4 vezes. Você pode ver isso no arquivo de log pelo número de vezes em que Windows is Ready to use é exibido.

```
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
Ec2Config service v2.1.9.0
RedHat PV NIC Driver v1.3.10.0
2013/03/15 17:11:01Z: Waiting for meta-data accessibility...
2013/03/15 17:11:02Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BF64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
<Username>Administrator</Username>
<Password>
L79ThJPF8LyIL38I2ht0FBrjet3vnT2csTiU/XGVMRCH7kQtBnznAnXrKdlsirXlx19BwVMsd9b38jFJqv01IUpgNNJRZoCDc7IbUw
</Password>
2013/03/15 17:11:30Z: Product activation was successful.
2013/03/15 17:11:32Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
Ec2Config service v2.1.9.0
2013/03/15 21:04:24Z: There was an exception writing driver information to console: System.Exception: 
at Ec2Config.Service1.Go()
2013/03/15 21:04:35Z: Waiting for meta-data accessibility...
2013/03/15 21:04:40Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BF64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:05:08Z: Product activation was successful.
2013/03/15 21:05:09Z: Message: Windows is Ready to use
Microsoft Windows NT 6.0.6002 Service Pack 2 (en-US)
Ec2Config service v2.1.9.0
Citrix PV Ethernet Adapter v5.9.960.49119
2013/03/15 21:07:20Z: Waiting for meta-data accessibility...
2013/03/15 21:07:21Z: Meta-data is now available.
<RDPCERTIFICATE>
<THUMBPRINT>D6BF64F21359516C781CA7DF2821C5EFC35648A</THUMBPRINT>
</RDPCERTIFICATE>
2013/03/15 21:07:27Z: Message: Windows is Ready to use
```

8. Conecte-se à instância e faça login como administrador local.
9. Feche a caixa de diálogo Desinstalador dos drivers Xen paravirtualizados Red Hat para Windows.
10. Verifique se a instalação foi concluída. Navegue até a pasta Citrix-WIN_PV que você extraiu anteriormente, abra o arquivo PVUpgrade.log e verifique o texto INSTALLATION IS COMPLETE.



```
PVUpgrade - Notepad
File Edit Format View Help
20130315_0905125 Reinstall Device PCI\IDE\IDECHANNEL\4&80005ED&0&0
20130315_0905133 Reinstall Device PCI\VEN_8086&DEV_7010&SUBSYS_00015853&REV_00\3&267A616A&0&0
20130315_0905141 Reinstall Device ACPI\PNP0A03\0
20130315_0905149 Removing Service: rhelfltr
20130315_0905149 Removing Service: rhelnet
20130315_0905149 Removing Service: rhelscsf
20130315_0905149 Removing Driver File: c:\windows\System32\drivers\rhelfltr.sys
20130315_0905150 Removing Driver File: C:\Windows\System32\drivers\rhelnet.sys
20130315_0905150 Removing Redhat Service: C:\Windows\System32\rhelsvc.exe
20130315_0905150 Unable to delete file, need to restart
20130315_0905150 -
20130315_0905150 Restarting computer...
20130315_0907105 START: 20130315_0907
20130315_0907105 Running as: SYSTEM
20130315_0907105 Current Running Directory: C:\Users\Administrator\Downloads\Citrix-WIN_PV
20130315_0907105 Detecting Windows Version
20130315_0907116 Reinstall Device PCI\IDE\IDECHANNEL\4&80005ED&0&1
20130315_0907141 Reinstall Device PCI\VEN_8086&DEV_7010&SUBSYS_00015853&REV_00\3&267A616A&0&0
20130315_0907149 Reinstall Device PCI\VEN_8086&DEV_7010&SUBSYS_00015853&REV_00\3&267A616A&0&0
20130315_0907157 Reinstall Device ACPI\PNP0A03\0
20130315_0908105 Removing Redhat Service: C:\Windows\System32\rhelsvc.exe
20130315_0908105 Removing Driver File: C:\Windows\System32\drivers\rhelscsf.sys
20130315_0908108 Adding Quick Removal Settings to: C:\Windows\System32\DriverStore\FileRepository\disk.inf_126712d3\disk
20130315_0908108 Adding First Surprise Removal Item
20130315_0908108 Adding Last Surprise Removal Item
20130315_0908108 Edits Saved
20130315_0908108 Setting Existing Disks for Quick Removal
20130315_0908108 Complete
20130315_0908108 Adding Quick Removal Settings to: C:\Windows\System32\DriverStore\FileRepository\disk.inf_5c850fad\disk
20130315_0908108 Adding First Surprise Removal Item
20130315_0908108 Adding Last Surprise Removal Item
20130315_0908108 Edits Saved
20130315_0908108 Setting Existing Disks for Quick Removal
20130315_0908108 Complete
20130315_0908108 Removing Scheduled Task
20130315_0908109
20130315_0908109 IMPORTANT: Please uninstall any remaining Redhat driver software from Add/Remove Programs
20130315_0908109
20130315_0908109 INSTALLATION IS COMPLETE
20130315_0908109 Setting Powershell script execution policy to Restricted
```

Atualizar o serviço de agente convidado do Citrix Xen

Se você estiver usando drivers Citrix PV no Windows Server, você poderá atualizar o serviço de agente de convidado do Citrix Xen. Esse serviço do Windows gerencia tarefas como eventos de desligamento e reinicialização a partir da API. Você pode executar esse pacote de atualização em qualquer versão do Windows Server, desde que a instância esteja executando drivers Citrix PV.

Important

Para Windows Server 2008 R2 e posterior, recomendamos atualizar para drivers AWS PV que incluem a atualização do agente convidado.

Antes de começar a atualizar seus drivers, faça backup de suas informações importantes sobre a instância ou crie uma AMI a partir da instância. Para obter mais informações sobre a criação de uma AMI, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#). Se você criar uma AMI, certifique-se de fazer o seguinte:

- Não habilite a ferramenta Sysprep no serviço EC2Config.
- Escreva sua senha.
- Defina o adaptador de Ethernet como DHCP.

Para atualizar seu serviço de agente convidado do Citrix Xen

1. Conecte-se à instância e faça login como administrador local. Para obter mais informações sobre como se conectar à sua instância, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
2. Em sua instância, [faça download](#) do pacote de atualização do Citrix.
3. Extraia o conteúdo dos pacotes de atualização para um local de sua escolha.
4. Clique duas vezes no arquivo Upgrade.bat. Se receber um aviso de segurança, selecione Executar.
5. Na caixa de diálogo Atualizar drivers, revise as informações e selecione Sim se você estiver pronto para iniciar a atualização.
6. Quando a atualização estiver concluída, o arquivo PVUpgrade.log será aberto e conterá o texto UPGRADE IS COMPLETE.
7. Reinicie a instância.

Solucionar problemas de drivers de PV

Veja a seguir soluções para problemas que podem ser encontrados com imagens do Amazon EC2 e drivers de PV mais antigos.

Tópicos

- [O Windows Server 2012 R2 perde a conectividade de rede e armazenamento após a reinicialização de uma instância \(p. 571\)](#)
- [Descarregamento de TCP \(p. 576\)](#)
- [Sincronização de horário \(p. 577\)](#)
- [Workloads que usam mais de 20.000 IOPS de disco apresentam degradação devido a gargalos da CPU \(p. 577\)](#)

[O Windows Server 2012 R2 perde a conectividade de rede e armazenamento após a reinicialização de uma instância](#)

Important

Esse problema ocorre somente com AMIs disponibilizadas antes de setembro de 2014.

As Imagens de máquina da Amazon (AMIs) do Windows Server 2012 R2 disponibilizadas antes de 10 de setembro de 2014 podem perder conectividade de rede e armazenamento após a reinicialização da instância. O erro no log do sistema do AWS Management Console indica: "Dificuldade em detectar detalhes do driver PV para a saída do console". A perda de conectividade é causada pelo recurso Limpeza de plug and play. Esse recurso verifica e desabilita dispositivos inativos do sistema a cada 30 dias. O recurso identifica incorretamente o dispositivo de rede EC2 como inativo e o remove do sistema. Quando isso ocorre, a instância perde a conectividade de rede após uma reinicialização.

Para sistemas que você suspeita estar sendo afetados por esse problema, é possível fazer download e executar uma atualização de driver no local. Caso não seja possível executar a atualização de driver no local, você pode executar um script auxiliar. O script determina se sua instância foi afetada. Se ela tiver sido afetada, e o dispositivo de rede do Amazon EC2 não tiver sido removido, o script desabilitará a verificação da Limpeza de plug and play. Se o dispositivo de rede tiver sido removido, o script reparará o dispositivo, desabilitará a verificação do recurso Limpeza de plug and play e permitirá que sua instância seja reinicializada com a conectividade de rede habilitada.

Tópicos

- [Escolher como corrigir problemas \(p. 572\)](#)
- [Método 1 – Redes aprimoradas \(p. 573\)](#)
- [Método 2 – Configuração do Registro \(p. 573\)](#)
- [Executar o script de correção \(p. 575\)](#)

[Escolher como corrigir problemas](#)

Há dois métodos para restaurar a conectividade de rede e de armazenamento em uma instância afetada por esse problema. Escolha um dos seguintes métodos:

Método	Pré-requisitos	Visão geral do procedimento
Método 1 – Redes aprimoradas	As redes aprimoradas só estão disponíveis em uma nuvem privada virtual (VPC) que exija um tipo de instância C3. Se o servidor não usar atualmente o tipo de instância C3, altere-o temporariamente.	Você altera o tipo de instância do servidor em uma instância C3. Em seguida, as redes aprimoradas permitem a você se conectar à instância afetada e corrigir o problema. Depois de corrigir o problema, você altera a instância de volta para o tipo original. Esse método é geralmente mais rápido do que o método 2 e tem menos probabilidade de resultar em erro do usuário. Haverá cobranças adicionais pelo período de execução da instância C3.
Método 2 – Configuração do Registro	Capacidade de criar ou acessar um segundo servidor. Capacidade de alterar as configurações do Registro.	Você desanexa o volume raiz da instância afetada, anexa-o a outra instância, conecta-se e faz alterações no Registro. Haverá cobranças adicionais pelo período de execução do servidor adicional. Esse método é mais lento do que o método 1, mas ele funcionou em situações nas quais o método 1 não resolveu o problema.

Método 1 – Redes aprimoradas

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize a instância afetada. Selecione a instância e escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância).

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Depois de interromper a instância, crie um backup. Selecione a instância e escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).
5. Altere o tipo de instância para qualquer tipo de instância C3.
6. Inicie a instância.
7. Conecte-se à instância usando o Desktop Remoto e [faça download](#) do pacote de atualização de drivers AWS PV na instância.
8. Extraia o conteúdo da pasta e execute `AWSPVDriverSetup.msi`.

Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza os drivers. A instância não estará disponível por até 15 minutos.

9. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se os novos drivers foram instalados. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do AWS PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte [AWSHistórico do pacote de drivers PV \(p. 561\)](#).
10. Interrompa a instância e altere-a de volta para seu tipo original.
11. Inicie a instância e retorne o uso normal.

Método 2 – Configuração do Registro

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Localize a instância afetada. Selecione a instância, escolha Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância).

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Escolha Launch instance (Executar instâncias) e crie uma instância temporária Windows Server 2008 ou Windows Server 2012 na mesma zona de disponibilidade que a instância afetada. Não crie uma instância Windows Server 2012 R2.

Important

Se você não criar a instância na mesma zona de disponibilidade que a instância afetada, não conseguirá associar o volume do dispositivo raiz da instância afetada à nova instância.

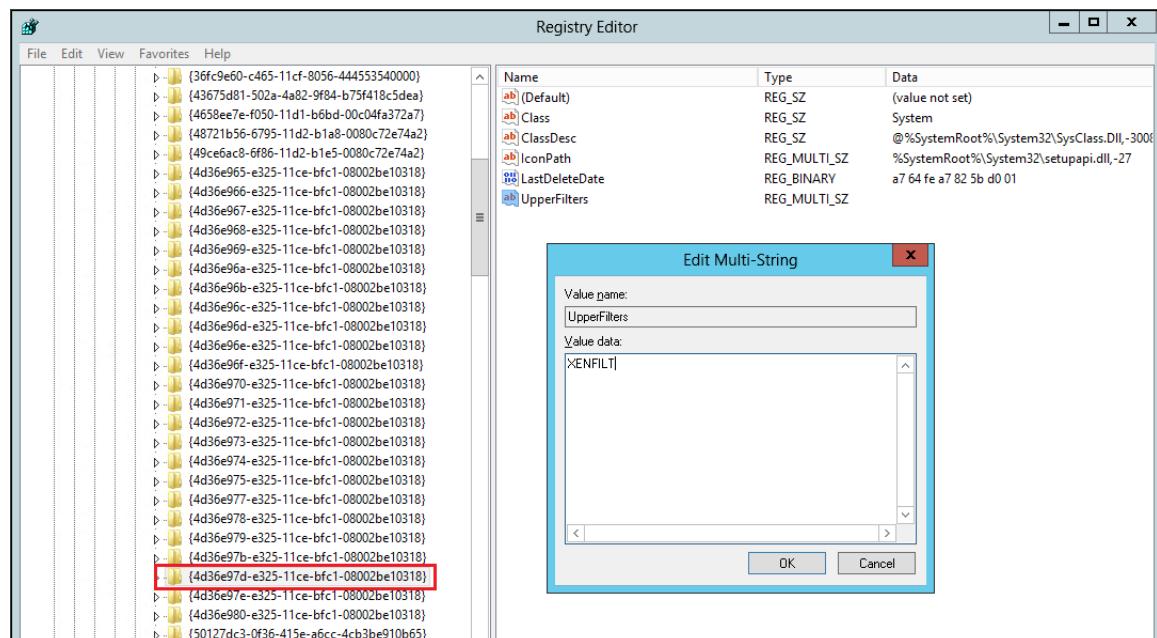
5. No painel de navegação, escolha Volumes.

6. Localize o volume do dispositivo raiz da instância afetada. [Desanexe o volume \(p. 1290\)](#) e [anexe o volume \(p. 1271\)](#) à instância temporária que você criou anteriormente. Associe-a com o nome do padrão do dispositivo (xvdf).
7. Use o Desktop Remoto para conectar-se à instância temporária e use em utilitário Gerenciamento de Disco para [disponibilizar o volume para uso \(p. 1272\)](#).
8. Na instância temporária, abra a caixa de diálogo Run (Executar), digite **regedit** e pressione Enter.
9. No painel de navegação do Editor de Registro, escolha HKEY_Local_Machine e no menu Arquivo escolha Carregar Hive.
10. Na caixa de diálogo Carregar Hive, navegue até Volume afetado\Windows\System32\config\System e digite um nome temporário na caixa de diálogo Nome da chave. Por exemplo, digite OldSys.
11. No painel de navegação do Editor de Registro, localize as seguintes chaves:

HKEY_LOCAL_MACHINE\your_temporary_key_name\ControlSet001\Control\Class\4d36e97d-e325-11ce-bfc1-08002be10318

HKEY_LOCAL_MACHINE\your_temporary_key_name\ControlSet001\Control\Class\4d36e96a-e325-11ce-bfc1-08002be10318

12. Para cada chave, clique duas vezes em UpperFilters, digite um valor de XENFILT e, em seguida, selecione OK.



13. Localize a seguinte chave:

HKEY_LOCAL_MACHINE\your_temporary_key_name\ControlSet001\Services\XENBUS\Parameters

14. Crie uma nova string (REG_SZ) com o nome ActiveDevice e o seguinte valor:

PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Localize a seguinte chave:

HKEY_LOCAL_MACHINE\your_temporary_key_name\ControlSet001\Services\XENBUS

16. Altere a contagem de 0 para 1.

17. Localize e exclua as seguintes chaves:

HKEY_LOCAL_MACHINE\your_temporary_key_name\ControlSet001\Services\xenvbd
\StartOverride

HKEY_LOCAL_MACHINE\your_temporary_key_name\ControlSet001\Services\xenfilt
\StartOverride

18. No painel de navegação do Editor de Registro, escolha a chave temporária que você criou quando abriu pela primeira vez o Editor de Registro.
19. No menu Arquivo, escolha Descarregar Hive.
20. No utilitário de Gerenciamento de Disco, escolha a unidade que você associou anteriormente, abra o menu contextual (botão direito do mouse) e escolha Offline.
21. No console do Amazon EC2, desanexe o volume afetado de instância temporária e reanexe-o à sua instância Windows Server 2012 R2 com o nome de dispositivo /dev/sda1. Você deve especificar o nome desse dispositivo para designar o volume como volume do dispositivo raiz.
22. **Inicie** a instância.
23. Conecte-se à instância usando o Desktop Remoto e [faça download](#) do pacote de atualização de drivers AWS PV na instância.
24. Extraia o conteúdo da pasta e execute `AWS PV Driver Setup.msi`.

Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza os drivers. A instância não estará disponível por até 15 minutos.

25. Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se os novos drivers foram instalados. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do AWS PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte [AWS Histórico do pacote de drivers PV \(p. 561\)](#).
26. Exclua ou interrompa a instância temporária que você criou nesse procedimento.

Executar o script de correção

Caso não seja possível executar uma atualização de driver no local nem migrar para uma instância mais nova, você pode executar o script de correção para corrigir os problemas causados pela tarefa da Limpeza de plug and play.

Para executar o script de correção

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Escolha a instância para a qual você deseja executar o script de correção. Escolha Instance State (Estado da instância) e, em seguida, escolha Stop Instance (Interromper instância).

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Depois de interromper a instância, crie um backup. Selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e, em seguida, escolha Create image (Criar imagem).
5. Escolha Instance state (Estado da instância) e, em seguida, escolha Start Instance (Iniciar instância).
6. Conecte-se à instância usando o Desktop Remoto e, em seguida, [faça download](#) da pasta RemediateDriverIssue.zip na instância.

7. Extraia o conteúdo da pasta.
8. Execute o script de correção de acordo com as instruções no arquivo Readme.txt. O arquivo está localizado na pasta onde você extraiu o RemediateDriverIssue.zip.

Descarregamento de TCP

Important

Esse problema não se aplica a instâncias que executam drivers de rede AWS PV ou Intel.

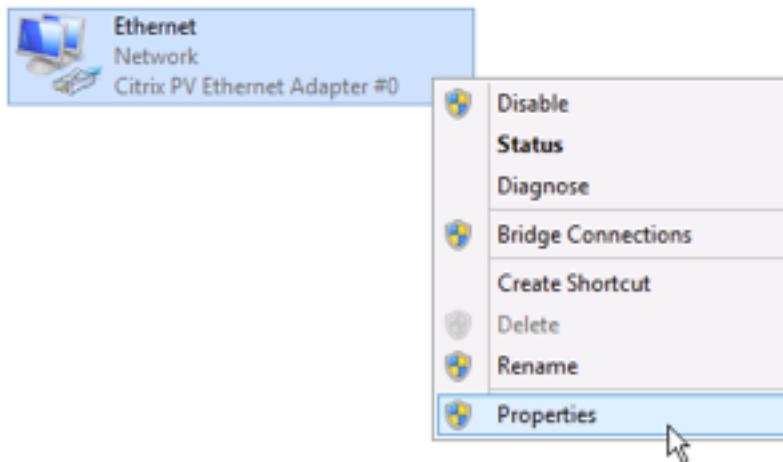
Por padrão, o descarregamento TCP é habilitado para os drivers Citrix PV em AMIs do Windows. Se você encontrar erros no nível do transporte ou na transmissão de pacotes (conforme esteja visível no monitor de performance do Windows)—por exemplo, quando você estiver executando determinadas workloads do SQL—talvez seja necessário desabilitar esse recurso.

Warning

Desabilitar o descarregamento TCP pode reduzir a performance de rede de sua instância.

Para desabilitar o descarregamento TCP para Windows Server 2012 e 2008

1. Conecte-se à instância e faça login como administrador local.
2. Se você estiver usando o Windows Server 2012, pressione Ctrl+Esc para acessar a tela Iniciar e, em seguida, selecione Painel de controle. Se você estiver usando o Windows Server 2008, escolha Iniciar e selecione Painel de controle.
3. Escolha Rede e Internet e, em seguida, Central de Rede e Compartilhamento.
4. Selecione Alterar configurações de adaptador.
5. Clique com o botão direito do mouse em Adaptador de rede Citrix PV Ethernet nº 0 e selecione Propriedades.



6. Na caixa de diálogo Propriedades de conexão de área local, selecione Configurar para abrir a caixa de diálogo Propriedades do adaptador Citrix PV Ethernet nº 0.
7. Na guia Avançado, desabilite cada uma das propriedades, exceto Valor correto da soma de verificação TCP/UDP. Para desabilitar uma propriedade, selecione-a em Propriedade e escolha Desabilitado em Valor.
8. Escolha OK.
9. Execute os comandos a seguir em uma janela do prompt de comando.

```
netsh int ip set global taskoffload=disabled
```

```
netsh int tcp set global chimney=disabled  
netsh int tcp set global rss=disabled  
netsh int tcp set global netdma=disabled
```

10. Reinicialize a instância.

Sincronização de horário

Antes da versão de 13/02/2013, a AMI do Windows, o agente convidado do Citrix Xen poderiam definir a hora do sistema incorretamente. Isso pode fazer com que seu locação de DHCP expire. Se você tiver problemas para se conectar à sua instância, talvez precise atualizar o agente.

Para determinar se você tem o agente convidado do Citrix Xen atualizado, verifique se a data do arquivo C:\Program Files\Citrix\XenGuestAgent.exe é a partir de março de 2013. Se a data nesse arquivo for anterior, atualize o serviço do agente convidado do Citrix Xen. Para obter mais informações, consulte [Atualizar o serviço de agente convidado do Citrix Xen \(p. 571\)](#).

Workloads que usam mais de 20.000 IOPS de disco apresentam degradação devido a gargalos da CPU

Você pode ser afetado por esse problema se estiver usando instâncias do Windows que executam os drivers AWS PV que usam mais de 20.000 IOPS, e se você encontrar o código 0x9E: USER_MODE_HEALTH_MONITOR de verificação de bugs.

As leituras e gravações de disco (E/S) nos drivers AWS PV ocorrem em duas fases: Preparação de E/S e Conclusão de E/S. Por padrão, a fase de preparação é executada em um único núcleo arbitrário. A fase de conclusão é executada no núcleo 0. A quantidade de computação necessária para processar uma E/S varia de acordo com o tamanho e outras propriedades. Algumas E/S usam mais computação na fase de preparação, e outras na fase de conclusão. Quando uma instância gera mais de 20.000 IOPS, a fase de preparação ou conclusão pode resultar em um gargalo, em que a CPU na qual ela é executada está com 100% de capacidade. Se a fase de preparação ou conclusão se torna ou não um gargalo depende das propriedades de E/S usadas pela aplicação.

Começando nos drivers AWS PV 8.4.0, a carga da fase de preparação e de conclusão podem ser distribuídas por vários núcleos, eliminando gargalos. Cada aplicação usa diferentes propriedades de E/S. Portanto, a adoção de uma das configurações a seguir pode aumentar, reduzir ou não afetar a performance da aplicação. Depois de aplicar qualquer uma dessas configurações, monitore a aplicação para verificar se ela está proporcionando a performance desejada.

1. Prerequisites

Antes de iniciar este procedimento de solução de problemas, verifique os seguintes pré-requisitos:

- A instância usa drivers AWS PV versão 8.4.0 ou posterior. Para atualizar, consulte [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#).
- Você tem acesso RDP à instância. Para conhecer as etapas para conectar-se à instância baseada no Windows usando RDP, consulte [Conectar-se à sua instância baseada no Windows usando RDP \(p. 444\)](#).
- Você tem acesso de administrador na instância.

2. Observe a carga da CPU na instância

Você pode usar o Gerenciador de Tarefas do Windows para exibir a carga em cada CPU, a fim de determinar possíveis gargalos na E/S do disco.

1. Verifique se a aplicação está executando e lidando com o tráfego semelhante à workload de produção.
2. Conecte-se à sua instância usando RDP.

3. Clique no menu Start (Iniciar) na sua instância.
 4. Insira Task Manager no menu Iniciar para abrir o Gerenciador de Tarefas.
 5. Se o Gerenciador de tarefas mostrar a exibição Summary (Resumo), clique em More details (Mais detalhes) para expandir a exibição detalhada.
 6. Escolha a guia Performance.
 7. Selecione a CPU no painel esquerdo.
 8. Clique com o botão direito do mouse no gráfico do painel principal e selecione Change graph to (Alterar gráfico para) > Logical processors (Processadores lógicos) para exibir cada núcleo individual.
 9. Dependendo de quantos núcleos estiverem na instância, com o passar do tempo você poderá ver linhas exibindo a carga da CPU, ou poderá ver somente um número.
 - Se forem exibidos gráficos da carga ao longo do tempo, procure CPUs onde a caixa esteja quase totalmente sombreada.
 - Se um número for exibido em cada núcleo, procure por núcleos que consistentemente mostrem 95% ou mais.
 10. Observe se o núcleo 0 ou um núcleo diferente está experimentando uma carga pesada.
3. Escolha qual configuração aplicar

Nome da configuração	Quando aplicar esta configuração	Observações
Default configuration	A workload está gerando menos de 20.000 IOPS, ou outras configurações não melhoraram a performance ou a estabilidade.	Para essa configuração, a E/S ocorre em alguns núcleos, o que pode beneficiar workloads menores, aumentando a localidade do cache e reduzindo a comutação de contexto.
Allow driver to choose whether to distribute completion	A workload está gerando mais de 20.000 IOPS e uma carga moderada ou alta é observada no núcleo 0.	Essa configuração é recomendada para todas as instâncias Xen que usam o PV 8.4.0 ou posterior, e que usam mais de 20.000 IOPS, independentemente de problemas serem encontrados ou não.
Distribute both preparation and completion	A workload está gerando mais de 20.000 IOPS. Ou a permissão para o driver escolher a distribuição não melhorou a performance, ou um núcleo diferente de 0 está experimentando uma alta carga.	Esta configuração permite a distribuição da preparação de E/S e da conclusão de E/S.

Note

Recomendamos que você não distribua a preparação de E/S sem também distribuir a conclusão de E/S (configuração DpcRedirection sem configuração NotifierDistributed) porque a fase de conclusão é sensível à sobrecarga na fase de preparação, quando a fase de preparação estiver ocorrendo em paralelo.

Valores de chave do Registro

- NotifierDistributed

Valor 0 ou não presente — A fase de conclusão será executada no núcleo 0.

Valor 1 — O driver escolhe executar a fase de conclusão, o núcleo 0 ou um núcleo adicional por disco conectado.

Valor 2 — O driver executa a fase de conclusão em um núcleo adicional por disco conectado.

- DpcRedirection

Valor 0 ou não presente — A fase de preparação será executada em um único núcleo arbitrário.

Valor 1 — A fase de preparação é distribuída entre vários núcleos.

Configuração padrão

Aplique a configuração padrão com as versões de driver AWS PV anteriores à 8.4.0 ou se a degradação da performance ou da estabilidade for observada após a aplicação de uma das outras configurações nesta seção.

1. Conecte-se à sua instância usando RDP.
2. Abra um novo prompt de comando do PowerShell como um administrador.
3. Execute os seguintes comandos para remover as chaves de registro **NotifierDistributed** e **DpcRedirection**.

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd\Parameters -  
Name NotifierDistributed
```

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd\Parameters -  
Name DpcRedirection
```

4. Reinicie a instância.

Permitir que o driver escolha se deseja distribuir a conclusão

Defina a chave de registro **NotifierDistributed** para permitir que o driver de armazenamento PV escolha se deve ou não distribuir a conclusão de E/S.

1. Conecte-se à sua instância usando RDP.
2. Abra um novo prompt de comando do PowerShell como um administrador.
3. Use o comando a seguir para adicionar a chave de registro **NotifierDistributed**.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd  
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Reinicie a instância.

Distribuir a preparação e a conclusão

Defina as chaves de registro `NotifierDistributed` e `DpcRedirection` para sempre distribuir as fases de preparação e conclusão.

1. Conecte-se à sua instância usando RDP.
2. Abra um novo prompt de comando do PowerShell como um administrador.
3. Execute os seguintes comandos para definir as chaves de registro `NotifierDistributed` e `DpcRedirection`.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Reinicie a instância.

AWSDrivers NVMe para instâncias do Windows

Os volumes do EBS e volumes de armazenamento de instâncias são expostos como dispositivos de blocos NVMe em [instâncias baseadas em Nitro \(p. 154\)](#). Você deve ter o driver AWS NVMe instalado para usar um dispositivo de blocos NVMe. As AMIs do Windows da AWS mais recentes para Windows Server 2008 R2 ou posterior contêm o driver AWS NVMe necessário.

Para obter mais informações sobre o EBS e o NVMe, consulte [Amazon EBS e NVMe em instâncias Windows \(p. 1438\)](#). Para obter mais informações sobre armazenamento de instâncias em SSD e o NVMe, consulte [Volumes de armazenamento de instâncias SSD \(p. 1503\)](#).

Instalar ou atualizar drivers AWS NVMe

Se você não está usando as AMIs do Windows da AWS mais recentes fornecidas pela Amazon, use o procedimento a seguir para instalar o driver AWS NVMe atual. Você deve executar essa atualização em um momento conveniente para reiniciar a instância. O script de instalação reiniciará sua instância ou você deverá reiniciá-la como a etapa final.

Pré-requisitos

PowerShell 3.0 ou posterior

Para fazer download e instalar o driver AWS NVMe mais recente

1. Recomendamos que você crie uma AMI como backup da seguinte forma, caso precise reverter suas alterações.
 - a. Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Antes de interromper uma instância, verifique se você copiou todos os dados necessários dos volumes de armazenamento de instâncias para um armazenamento persistente, como o Amazon EBS ou o Amazon S3.
 - b. No painel de navegação, escolha Instances (Instâncias).
 - c. Selecione a instância que requer a atualização do driver e escolha Instance state (Estado da instância), Stop Instance (Parar instância).
 - d. Depois que a instância for interrompida, selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos) e escolha Create image (Criar imagem).

- e. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).
2. Conecte-se à instância e faça login como administrador local.
3. Faça download e extraia os drivers para sua instância usando uma das seguintes opções:
 - Usando um navegador:
 - a. Faça download do pacote de drivers mais recente na instância.
 - b. Extraia o arquivo zip.
 - Usando o PowerShell:

```
invoke-webrequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/Latest/AWSNVMe.zip -outfile $env:USERPROFILE\ nvme_driver.zip expand-archive $env:UserProfile\ nvme_driver.zip -DestinationPath $env:UserProfile\ nvme_driver
```
4. Instale o driver em sua instância executando o script do PowerShell `install.ps1` do diretório `nvme_driver` (`.\install.ps1`). Se você receber um erro, verifique se está usando o PowerShell 3.0 ou posterior.
5. Se o instalador não reinicializar sua instância, reinicie-a.

AWSHistórico da versão do driver NVMe

A tabela a seguir descreve as versões lançadas do driver AWS NVMe.

Versão do driver	Detalhes	Data de lançamento
1.3.2	Corrigido o problema com a modificação de volumes do EBS processando a E/S ativamente, o que pode resultar em dados corrompidos. Os clientes que não modificam volumes do EBS online (por exemplo, redimensionando ou alterando o tipo) não são afetados.	10 de setembro de 2019
1.3.1	Melhorias na confiabilidade	21 de maio de 2019
1.3.0	Melhorias de otimização do dispositivo	31 de agosto de 2018
1.2.0	Melhorias na performance e confiabilidade para dispositivos NVMe da AWS em todas as instâncias compatíveis, incluindo instâncias bare metal.	13 de junho de 2018
1.0.0	AWSDriver NVMe para tipos de instâncias compatíveis executando Windows Server	12 de fevereiro de 2018

Assinar notificações do

O Amazon SNS pode notificá-lo quando novas versões dos drivers EC2 para Windows são lançadas. Use o procedimento a seguir para se inscrever nessas notificações.

Como assinar as notificações do EC2 no console

1. Abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.

2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região porque as notificações do SNS que você está assinando estão nesta região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
 - a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):
`arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers`
 - b. Para Protocolo, selecione Email.
 - c. Para Endpoint, digite um endereço de e-mail que você pode usar para receber as notificações.
 - d. Selecione Create subscription.
6. Você receberá um e-mail de confirmação. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que novos drivers EC2 para Windows são lançados, nós enviamos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações do driver Amazon EC2 para Windows

1. Abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.
2. No painel de navegação, escolha Subscriptions.
3. Selecione a caixa de seleção para a assinatura e, depois, escolha Ações, Excluir assinaturas. Quando a confirmação for solicitada, escolha Excluir.

Para assinar as notificações do EC2 usando a AWS CLI

Para assinar as notificações do EC2 com a AWS CLI, use o comando a seguir.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --  
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Para assinar as notificações do EC2 usando o AWS Tools for Windows PowerShell

Para assinar as notificações do EC2 com AWS Tools for Windows PowerShell, use o comando a seguir.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers'  
-Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Otimizar as opções de CPU

As instâncias do Amazon EC2 oferecem suporte a multithreading, que permite a execução de vários threads simultaneamente em um único núcleo de CPU. Cada thread é representado como uma CPU virtual (vCPU) na instância. Uma instância tem um número padrão de núcleos de CPU, que varia de acordo com o tipo de instância. Por exemplo, um tipo de instância m5.xlarge tem dois núcleos de CPU e dois threads por núcleo por padrão—: quatro vCPUs no total.

Note

Cada vCPU é um thread de um núcleo de CPU, exceto instâncias T2 e instâncias desenvolvidas por processadores AWS Graviton2.

Na maioria dos casos, há um tipo de instância do Amazon EC2 que tem uma combinação de memória e número de vCPUs para atender às suas workloads. No entanto, você pode especificar as seguintes opções de CPU para otimizar a instância para workloads ou necessidades de negócios específicas:

- Número de núcleos de CPU: você pode personalizar o número de núcleos de CPU para a instância. Você pode fazer isso para otimizar potencialmente os custos de licenciamento do software com uma instância que tem quantidade de RAM suficiente para workloads com uso intensivo de memória, mas menos núcleos de CPU.
- Threads por núcleo: você pode desabilitar o multithreading especificando um único thread por núcleo de CPU. Você pode fazer isso para determinadas workloads, como workloads de computação de alta performance (HPC).

Você pode especificar essas opções de CPU durante a execução da instância. Não há cobrança adicional ou reduzida para especificar opções de CPU. Você será cobrado da mesma forma das instâncias executadas com opções de CPU padrão.

Tópicos

- [Regras para especificar opções de CPU \(p. 583\)](#)
- [Núcleos de CPU e threads por núcleo de CPU por tipo de instância \(p. 583\)](#)
- [Especificar opções de CPU para a instância \(p. 598\)](#)
- [Visualizar as opções de CPU para a instância \(p. 600\)](#)

Regras para especificar opções de CPU

Para especificar as opções de CPU para a instância, lembre-se das seguintes regras:

- As opções de CPU podem ser especificadas somente durante a execução da instância e não podem ser alteradas após a execução.
- Ao executar uma instância, você deve especificar o número de núcleos de CPU e threads por núcleo na solicitação. Por obter exemplos de solicitação, consulte [Especificar opções de CPU para a instância \(p. 598\)](#).
- O número total de vCPUs para a instância é o número de núcleos de CPU multiplicado pelos threads por núcleo. Para especificar um número personalizado de vCPUs, você deve especificar um número válido de núcleos de CPU e threads por núcleo para o tipo de instância. Você não pode exceder o número padrão de vCPUs para a instância. Para obter mais informações, consulte [Núcleos de CPU e threads por núcleo de CPU por tipo de instância \(p. 583\)](#).
- Para desabilitar o multithreading, especifique um thread por núcleo.
- Quando você [altera o tipo de instância \(p. 244\)](#) de uma instância existente, as opções de CPU são alteradas automaticamente para as opções de CPU padrão no novo tipo de instância.
- As opções de CPU especificadas depois de você interromper, iniciar ou reiniciar uma instância.

Núcleos de CPU e threads por núcleo de CPU por tipo de instância

As tabelas a seguir listam os tipos de instância que oferecem suporte à especificação de opções de CPU.

Tópicos

- [Instâncias computacionais aceleradas \(p. 584\)](#)
- [Instâncias otimizadas para computação \(p. 585\)](#)
- [Instâncias de uso geral \(p. 587\)](#)

- [Instâncias otimizadas para memória \(p. 592\)](#)
- [Instâncias otimizadas para armazenamento \(p. 597\)](#)

Instâncias computacionais aceleradas

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
f1.2xlarge	8	4	2	1 a 4	1, 2
f1.4xlarge	16	8	2	1 a 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g3.4xlarge	16	8	2	1 a 8	1, 2
g3.8xlarge	32	16	2	1 a 16	1, 2
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g3s.xlarge	4	2	2	1, 2	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	1, 2	1, 2
g4dn.2xlarge	8	4	2	1 a 4	1, 2
g4dn.4xlarge	16	8	2	1 a 8	1, 2
g4dn.8xlarge	32	16	2	1 a 16	1, 2
g4dn.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p2.xlarge	4	2	2	1, 2	1, 2
p2.8xlarge	32	16	2	1 a 16	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
p2.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3.2xlarge	8	4	2	1 a 4	1, 2
p3.8xlarge	32	16	2	1 a 16	1, 2
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instâncias otimizadas para computação

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c4.large	2	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1 a 4	1, 2
c4.4xlarge	16	8	2	1 a 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20,	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				22, 24, 26, 28, 30, 32, 34, 36	
c5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1 a 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1 a 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Instâncias de uso geral

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1 a 4	1, 2
m4.4xlarge	16	8	2	1 a 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5ad.large	2	1	2	1	1, 2
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2
m5dn.xlarge	4	2	2	2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	2	1, 2
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5n.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
t2.nano	1	1	1	1	1
t2.micro	1	1	1	1	1
t2.small	1	1	1	1	1
t2.medium	2	2	1	1, 2	1
t2.large	2	2	1	1, 2	1
t2.xlarge	4	4	1	1 a 4	1
t2.2xlarge	8	8	1	1 a 8	1
t3.nano	2	1	2	1	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
t3.micro	2	1	2	1	1, 2
t3.small	2	1	2	1	1, 2
t3.medium	2	1	2	1	1, 2
t3.large	2	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2	1	2	1	1, 2
t3a.micro	2	1	2	1	1, 2
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2

Instâncias otimizadas para memória

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1 a 4	1, 2
r4.4xlarge	16	8	2	1 a 8	1, 2
r4.8xlarge	32	16	2	1 a 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5ad.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2
r5b.xlarge	4	2	2	2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5b.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2
r5dn.xlarge	4	2	2	2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	2	1, 2
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r5n.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
u-6tb1.56xlarge	224	224	1	1 a 224	1
u-6tb1.112xlarge	448	224	2	1 a 224	1, 2
u-9tb1.112xlarge	448	224	2	1 a 224	1, 2
u-12tb1.112xlarge	448	224	2	1 a 224	1, 2
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1 a 4	1, 2
x1e.4xlarge	16	8	2	1 a 8	1, 2
x1e.8xlarge	32	16	2	1 a 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
z1d.large	2	1	2	1	1, 2
z1d.xlarge	4	2	2	2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Instâncias otimizadas para armazenamento

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1 a 4	1, 2
d2.4xlarge	16	8	2	1 a 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.large	2	1	2	1	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1 a 4	1, 2
h1.4xlarge	16	8	2	1 a 8	1, 2
h1.8xlarge	32	16	2	1 a 16	1, 2
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18,	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				20, 22, 24, 26, 28, 30, 32	
i3.large	2	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1 a 4	1, 2
i3.4xlarge	16	8	2	1 a 8	1, 2
i3.8xlarge	32	16	2	1 a 16	1, 2
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
i3en.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Especificar opções de CPU para a instância

Você pode especificar as opções de CPU durante a execução da instância. Os seguintes exemplos são para um tipo de instância `r4.4xlarge`, que tem os seguintes [valores padrão \(p. 592\)](#):

- Núcleos de CPU padrão: 8
- Threads padrão por núcleo: 2
- vCPUs padrão: 16 (8 x 2)
- Número válido de núcleos de CPU: 1, 2, 3, 4, 5, 6, 7, 8
- Número válido de threads por núcleo: 1, 2

Desativar multithreading

Para desabilitar o multithreading, especifique um thread por núcleo.

Como desabilitar o multithreading durante a execução da instância (console)

1. Siga o procedimento do [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).
2. Na página Configure Instance Details (Configurar detalhes da instância), em CPU options (Opções de CPU), escolha Specify CPU options (Especificar opções de CPU).
3. Em Core count (Contagem de núcleos), defina o número de núcleos de CPU necessário. Neste exemplo, para especificar a contagem de núcleos de CPU para uma instância **r4.4xlarge**, escolha 8.
4. Para desabilitar o multithreading, em Threads per core (Threads por núcleo), escolha 1.
5. Continue como solicitado pelo assistente. Ao terminar de revisar suas opções na página Review Instance Launch (Revisar execução da instância), selecione Launch (Executar). Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).

Como desabilitar o multithreading durante a execução da instância (AWS CLI)

Use o comando `run-instances` da AWS CLI e especifique um valor de 1 para `ThreadsPerCore` no parâmetro `--cpu-options`. Em `CoreCount`, especifique o número de núcleos de CPU. Neste exemplo, para especificar a contagem de núcleos de CPU padrão para uma instância **r4.4xlarge**, especifique um valor de 8.

```
aws ec2 run-instances --image-id ami-1a2b3c4d --instance-type r4.4xlarge --cpu-options "CoreCount=8,ThreadsPerCore=1" --key-name MyKeyPair
```

Especificando um número personalizado de vCPUs

Você pode personalizar o número de núcleos de CPU e de thread por núcleo da instância.

Para especificar um número personalizado de vCPUs durante a execução da instância (console)

O exemplo a seguir executa uma instância **r4.4xlarge** com seis vCPUs.

1. Siga o procedimento do [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).
2. Na página Configure Instance Details (Configurar detalhes da instância), em CPU options (Opções de CPU), escolha Specify CPU options (Especificar opções de CPU).
3. Para obter seis vCPUs, especifique três núcleos de CPU e dois threads por núcleo, da seguinte forma:
 - Para Core count (Contagem de núcleos), escolha 3.
 - For Threads per core (Threads por núcleo), escolha 2.
4. Continue como solicitado pelo assistente. Ao terminar de revisar suas opções na página Review Instance Launch (Revisar execução da instância), selecione Launch (Executar). Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).

Para especificar um número personalizado de vCPUs durante a execução da instância (AWS CLI)

O exemplo a seguir executa uma instância **r4.4xlarge** com seis vCPUs.

Use o comando [run-instances](#) da AWS CLI e especifique o número de núcleos de CPU e o número de threads no parâmetro `--cpu-options`. Você pode especificar três núcleos de CPU e dois threads por núcleo para obter seis vCPUs.

```
aws ec2 run-instances --image-id ami-1a2b3c4d --instance-type r4.4xlarge --cpu-options  
"CoreCount=3,ThreadsPerCore=2" --key-name MyKeyPair
```

Se preferir, especifique seis núcleos de CPU e um thread por núcleo (desabilite o multithreading) para obter seis vCPUs:

```
aws ec2 run-instances --image-id ami-1a2b3c4d --instance-type r4.4xlarge --cpu-options  
"CoreCount=6,ThreadsPerCore=1" --key-name MyKeyPair
```

Visualizar as opções de CPU para a instância

Você pode visualizar as opções de CPU de uma instância existente no console do Amazon EC2 ou descrevendo a instância usando a AWS CLI.

New console

Para visualizar as opções de CPU para uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação à esquerda, escolha Instances (Instâncias) e selecione a instância.
3. Na guia Details (Detalhes), em Host and placement group (Host e placement group), localizeNumber of vCPUs (Número de vCPUs).
4. Para visualizar a contagem de núcleos e de threads por núcleo, escolha o valor de Number of vCPUs (Número de vCPUs).

Old console

Para visualizar as opções de CPU para uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação à esquerda, escolha Instances (Instâncias) e selecione a instância.
3. Escolha Description (Descrição) e localize Number of vCPUs (Número de vCPUs).
4. Para visualizar a contagem de núcleos e de threads por núcleo, escolha o valor de Number of vCPUs (Número de vCPUs).

Para visualizar as opções de CPU de uma instância (AWS CLI)

Use o comando [describe-instances](#).

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

```
...  
"Instances": [  
    {  
        "Monitoring": {  
            "State": "disabled"  
        },  
        "PublicDnsName": "ec2-198-51-100-5.eu-central-1.compute.amazonaws.com",  
        "State": {  
            "Code": 16,
```

```
        "Name": "running"
    },
    "EbsOptimized": false,
    "LaunchTime": "2018-05-08T13:40:33.000Z",
    "PublicIpAddress": "198.51.100.5",
    "PrivateIpAddress": "172.31.2.206",
    "ProductCodes": [],
    "VpcId": "vpc-1a2b3c4d",
    "CpuOptions": {
        "CoreCount": 34,
        "ThreadsPerCore": 1
    },
    "StateTransitionReason": "",
    ...
}
]
```

Na saída que é retornada, o campo `CoreCount` indica o número de núcleos para a instância. O campo `ThreadsPerCore` indica o número de threads por núcleo.

Se preferir, conecte-se à instância e use uma ferramenta do Gerenciador de tarefas, para visualizar as informações de CPU para a instância.

Você pode usar o AWS Config para fazer registros, auditorias e avaliações de alterações de configuração para instâncias, incluindo instâncias encerradas. Para obter mais informações, consulte [Conceitos básicos do AWS Config](#) no Guia do desenvolvedor do AWS Config .

Definir o horário para uma instância do Windows.

Uma referência de tempo consistente e precisa é crucial para muitas tarefas e processos de servidor. A maioria dos logs do sistema incluem um time stamp que você pode usar para determinar quando os problemas ocorrem e em que ordem os eventos acontecem. Se você usar um SDK da AWS CLI ou da AWS para fazer solicitações de sua instância, essas ferramentas assinarão solicitações em seu nome. Se a data e a hora da sua instância não estiverem definidas corretamente, a data na assinatura poderá não corresponder à data da solicitação, e a AWS rejeitará a solicitação.

A Amazon fornece o Amazon Time Sync Service, que é acessível de todas as instâncias do EC2 e também é usado por outros serviços da AWS. Esse serviço utiliza uma frota de relógios atômicos de referência conectados via satélite em cada região para fornecer leituras de hora atuais e precisas do padrão global de Tempo Universal Coordenado (UTC) por meio do Network Time Protocol (NTP). O Amazon Time Sync Service suaviza automaticamente qualquer segundo bissexto adicionado ao UTC.

O Amazon Time Sync Service está disponível por meio do NTP no endereço IPv4 169.254.169.123 ou no endereço IPv6 fd00:ec2::123 para todas as instâncias em execução em uma VPC. Sua instância não requer acesso à Internet, e você não precisa configurar suas regras de security group nem de network ACL para permitir o acesso. As versões mais recentes das AMIs do Windows na AWS são sincronizadas com o Amazon Time Sync Service por padrão.

Note

Os exemplos nesta seção usam o endereço IPv4 do Amazon Time Sync Service: 169.254.169.123. Se você estiver recuperando tempo para instâncias do EC2 sobre o endereço IPv6, certifique-se de usar o endereço IPv6: fd00:ec2::123. O endereço IPv6 só é acessível no [Instâncias criadas no Sistema Nitro \(p. 154\)](#).

Devo usar UTC para minhas instâncias?

Recomendamos que você use o Tempo Universal Coordenado (UTC) para suas instâncias, a fim de evitar erros humanos e facilitar a sincronização em todos os CloudWatch logs, métricas, logs locais e outros

serviços. No entanto, você pode optar por usar um fuso horário diferente para melhor atender às suas necessidades.

Quando você usar fusos horários locais em vez de UTC, considere aspectos como horário de verão (quando aplicável) para automação, código, trabalhos agendados, atividades de solução de problemas (que correlacionam registros) e muito mais.

Use os procedimentos a seguir para configurar o Amazon Time Sync Service na sua instância usando o prompt de comando. Se preferir, você também pode usar fontes de NTP externas. Para obter mais informações sobre NTP e fontes públicas de hora, consulte <http://www.ntp.org/>. Uma instância precisa ter acesso à Internet para que as fontes de hora de NTP externas funcionem.

Para instâncias do Linux, consulte [Definir o horário da sua instância do Linux](#).

Tópicos

- [Alterar o fuso horário \(p. 602\)](#)
- [Configurar NTP \(Network Time Protocol\) \(p. 602\)](#)
- [Configurações de NTP \(Network Time Protocol\) padrão para AMIs do Windows da Amazon \(p. 603\)](#)
- [Configurar definições de horário para o Windows Server 2008 e posterior \(p. 604\)](#)
- [Recursos relacionados \(p. 605\)](#)

Alterar o fuso horário

As instâncias do Windows estão definidas para o fuso horário UTC por padrão. É possível alterar o horário para corresponder a seu fuso horário local ou a um fuso horário de outra parte da rede.

Para alterar o fuso horário de uma instância

1. Na instância, abra uma janela de prompt de comando.
2. Identifique o fuso horário a ser usado na instância. Para obter uma lista de fusos horários, use o seguinte comando: `tzutil /l`. Esse comando retorna uma lista com todos os fusos horários disponíveis usando o seguinte formato:

```
display name
time zone ID
```

3. Localize o ID do fuso horário a ser atribuído à instância.
4. Atribua o fuso horário à instância usando o seguinte comando:

```
tzutil /s "Pacific Standard Time"
```

O novo fuso horário deve entrar em funcionamento imediatamente.

Configurar NTP (Network Time Protocol)

A Amazon fornece o Amazon Time Sync Service, que é acessível de todas as instâncias do EC2 e também é usado por outros serviços da AWS. Recomendamos que você configure a instância para usar o Amazon Time Sync Service. Esse serviço utiliza uma frota de relógios de referência atômica conectados via satélite em cada região da AWS para fornecer leituras de hora atuais e precisas do padrão global de Tempo Universal Coordenado (UTC). O Amazon Time Sync Service suaviza automaticamente qualquer segundo bissexto adicionado ao UTC. Esse serviço está disponível no endereço IPv4 169.254.169.123 ou no endereço IPv6 fd00:ec2::123 para qualquer instância em execução em uma VPC, e sua instância não precisa de acesso à Internet para usar esse serviço. A versão das AMIs do Windows de agosto de 2018 em diante usam o Amazon Time Sync Service por padrão.

Para verificar a configuração de NTP

1. Na instância, abra uma janela de prompt de comando.
2. Obtenha a configuração de NTP atual digitando o seguinte comando:

```
w32tm /query /configuration
```

Esse comando retorna as definições de configuração atuais para a instância do Windows.

3. (Opcional) Obtenha o status da configuração atual digitando o seguinte comando:

```
w32tm /query /status
```

Esse comando retorna informações, como o último horário em que a instância foi sincronizada com o servidor NTP e o intervalo de sondagem.

Para alterar o servidor NTP para usar o Amazon Time Sync Service

1. Na janela de prompt de comando, execute o seguinte comando:

```
w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
```

2. Verifique suas novas configurações usando o seguinte comando:

```
w32tm /query /configuration
```

No resultado retornado, verifique se `NtpServer` exibe o endereço IP 169.254.169.123.

É possível alterar a instância para usar um conjunto diferente de servidores NTP, se necessário. Por exemplo, se houver instâncias do Windows sem acesso à Internet, configure-as para usar um servidor NTP localizado na sua rede privada. Se a instância estiver dentro de um domínio, você deve alterar as configurações para usar os controladores de domínio como a fonte de horário para evitar distorção de tempo. O grupo de segurança de sua instância deve ser configurado para permitir tráfego UDP de saída na porta 123 (NTP).

Para alterar os servidores NTP

1. Na janela de prompt de comando, execute o seguinte comando:

```
w32tm /config /manualpeerlist:"NTP servers" /syncfromflags:manual /update
```

Em que **NTP servers** (Servidores NTP) é a lista de servidores NTP delimitada por espaço para a instância usar.

2. Verifique suas novas configurações usando o seguinte comando:

```
w32tm /query /configuration
```

Configurações de NTP (Network Time Protocol) padrão para AMIs do Windows da Amazon

As Imagens de máquina da Amazon (AMIs) geralmente aderem aos padrões prontos para uso, exceto em casos em que alterações são necessárias para que funcionem na infraestrutura do EC2. As seguintes

configurações foram determinadas para funcionar de maneira adequada em um ambiente virtual, bem como manter qualquer desvio de relógio dentro um segundo de precisão:

- Intervalo de atualização: governa a frequência com que o serviço de tempo ajustará o tempo do sistema para a precisão. A AWS configura o intervalo de atualização para ocorrer uma vez a cada dois minutos.
- Servidor NTP – a partir da versão de agosto de 2018, as AMIs agora usam o serviço de horário da AWS por padrão. Esse serviço de horário pode ser acessado de qualquer região do EC2 no endpoint de 169.254.169.123. Além disso, o sinalizador 0x9 indica que o serviço de horário está atuando como um cliente e utiliza o `SpecialPollInterval` para determinar a frequência com a qual realizar verificações com o servidor de horário configurado.
- Tipo – "NTP" significa que o serviço atua como um cliente NTP autônomo em vez de agir como parte de um domínio.
- Habilitado e InputProvider – o serviço de horário está habilitado e fornece o horário ao sistema operacional.
- Intervalo de sondagem especial – realiza uma verificação com base no servidor NTP configurado a cada 900 segundos ou 15 minutos.

Caminho de registro	Nome da chave	Dados
HKLM:\System\CurrentControlSet\services\w32time\Config	UpdateInterval	120
HKLM:\System\CurrentControlSet\services\w32time\Parameters	NtpServer	169.254.169.123,0x9
HKLM:\System\CurrentControlSet\services\w32time\Parameters	Tipo	NTP
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\INtpClient	Enabled	1
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\INtpClient	InputProvider	1
HKLM:\System\CurrentControlSet\services\w32time\TimeProviders\INtpClient	SpecialPollInterval	900

Configurar definições de horário para o Windows Server 2008 e posterior

Quando você alterar o horário em uma instância do Windows, deverá garantir que o horário seja mantido durante as reinicializações de sistema. Caso contrário, quando a instância for reiniciada, ela voltará a usar o horário UTC. Para o Windows Server 2008 e versões posteriores, você pode manter o horário adicionando a chave de Registro `RealTimelsUniversal`. Essa chave é definida por padrão em todas as instâncias da geração atual. Para verificar se a chave `RealTimelsUniversal` do Registro está definida,

consulte a Etapa 4 no procedimento a seguir. Se a chave não estiver definida, siga estas etapas desde o início.

Para definir a chave do Registro RealTimelsUniversal

1. Na instância, abra uma janela de prompt de comando.
2. Use o seguinte comando para adicionar a chave de Registro:

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /v  
RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. Se estiver usando uma AMI do Windows Server 2008 (não do Windows Server 2008 R2) que tenha sido criada antes de 22 de fevereiro de 2013, recomendamos que você atualize para a versão mais recente da AMI do Windows da AWS. Se estiver usando uma AMI que executa o Windows Server 2008 R2 (não o Windows Server 2008), você deverá verificar se o hotfix da Microsoft [KB2922223](#) está instalado. Se esse hotfix não estiver instalado, recomendamos atualizar para o AMI mais recente do Windows da AWS.
4. (Opcional) Verifique se a instância salvou a chave com êxito usando o seguinte comando:

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /s
```

Esse comando retorna as subchaves da chave de Registro TimeZoneInformation. Você deve ver a chave RealTimelsUniversal na parte inferior da lista, semelhante à chave a seguir:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation		
Bias	REG_DWORD	0x1e0
DaylightBias	REG_DWORD	0xfffffffffc4
DaylightName	REG_SZ	@tzres.dll,-211
DaylightStart	REG_BINARY	00000300020002000000000000000000
StandardBias	REG_DWORD	0x0
StandardName	REG_SZ	@tzres.dll,-212
StandardStart	REG_BINARY	00000B00010002000000000000000000
TimeZoneKeyName	REG_SZ	Pacific Standard Time
DynamicDaylightTimeDisabled	REG_DWORD	0x0
ActiveTimeBias	REG_DWORD	0x1a4
RealTimeIsUniversal	REG_DWORD	0x1

Recursos relacionados

Para obter mais informações sobre como o sistema operacional Windows coordena e gerencia horários, incluindo a adição de um segundo bissexto, consulte a seguinte documentação:

- [Como funciona o serviço de tempo do Windows](#) (Microsoft)
- [W32tm](#) (Microsoft)
- [Como o serviço de tempo do Windows lida com o segundo bissexto](#) (Microsoft)
- [A história por trás dos segundos bissextos e do Windows: provavelmente não é Y2K](#) (Microsoft)

Definir a senha para uma instância do Windows

Quando se conectar a uma instância Windows, você deve especificar uma conta de usuário e uma senha que tenha permissão para acessar a instância. A primeira vez que se conectar a uma instância, será solicitado que você especifique a conta de administrador e a senha padrão.

Com as AMIs do Windows da AWS para o Windows Server 2012 R2 e anteriores, o serviço [EC2Config \(p. 530\)](#) gera uma senha padrão. Com as AMIs do Windows da AWS para o Windows Server 2016 e posterior, o [EC2Launch \(p. 522\)](#) gera uma senha padrão.

Note

Com o Windows Server 2016 e posterior, a opção `Password never expires` é desabilitada para o administrador local. Com o Windows Server 2012 R2 e anteriores, a opção `Password never expires` é habilitada para o administrador local.

Alterar a senha de administrador após a conexão

Quando você se conectar a uma instância pela primeira vez, recomendamos alterar a senha de administrador de seu valor padrão. Use o procedimento a seguir para alterar a senha de administrador para uma instância Windows.

Important

Armazene a nova senha em um lugar seguro. Você não poderá recuperar a nova senha usando o console do Amazon EC2. O console só pode recuperar a senha padrão. Se você tentar se conectar à instância usando a senha padrão depois de alterá-la, será exibido o erro "Suas credenciais não funcionaram".

Para alterar a senha de administrador local

1. Conecte-se à instância e abra o prompt de comando.
2. Execute o seguinte comando. Se sua nova senha incluir caracteres especiais, coloque a senha entre aspas duplas.

```
net user Administrator "new_password"
```

3. Armazene a nova senha em um lugar seguro.

Alterar uma senha perdida ou expirada

Se a senha for perdida ou expirar, você poderá gerar uma nova senha. Para obter os procedimentos de redefinição de senha, consulte [Redefinir uma senha de administrador do Windows perdida ou expirada \(p. 1590\)](#).

Adicionar componentes do Windows usando mídia de instalação

Os sistemas operacionais do Windows Server incluem muitos componentes opcionais. Não é prático incluir todos os componentes opcionais em cada AMI do Windows Server do Amazon EC2. Em vez disso, nós fornecemos a você snapshots do EBS de mídia de instalação que têm os arquivos necessários para configurar ou instalar componentes em sua instância do Windows.

Para acessar e instalar os componentes adicionais, você deve encontrar o snapshot do EBS correto para sua versão do Windows Server, criar um novo volume do snapshot e anexar o volume à sua instância.

Antes de começar

Use o AWS Management Console ou a ferramenta de linha de comando para obter o ID da instância e a zona de disponibilidade de sua instância. Você deve criar seu volume do EBS na mesma zona de disponibilidade de sua instância.

Adicionar componentes do Windows usando o console

Use o seguinte procedimento para usar o AWS Management Console para adicionar componentes do Windows à sua instância.

Para adicionar componentes do Windows à sua instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Snapshots.
3. Na barra Filter (Filtro), escolha Public Snapshots (Snapshots públicos).
4. Adicione o filtro Owner e escolha Amazon images.
5. Adicione o filtro Descrição e digite **Windows**.
6. Pressione Enter
7. Selecione o snapshot que corresponde à arquitetura do sistema e seu idioma de preferência. Por exemplo, selecione Windows 2019 English Installation Media se sua instância estiver executando o Windows Server 2019.
8. Escolha Ações, Criar volume.
9. Para Availability Zone (Zona de disponibilidade), selecione a zona de disponibilidade que corresponde à instância do Windows. Escolha Add Tag (Adicionar tag) e especifique **Name** para a chave de tag e um nome descritivo para o valor da tag. Escolha Create Volume (Criar volume).
10. Na mensagem Volume Successfully Created, escolha o volume que você acabou de criar.
11. Escolha Ações, Anexar volume.
12. Digite o ID da instância e o nome do dispositivo para o anexo e escolha Attach (Anexar). Se precisar de ajuda com o nome do dispositivo, consulte [Nomenclatura de dispositivos](#).
13. Conecte-se à sua instância e disponibilize o volume. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#).

Important

Não inicialize o volume.

14. Abra o Painel de Controle, Programas e Recursos. Escolha Ativar ou desativar recursos do Windows. Se for solicitado pela mídia de instalação, especifique o volume do EBS com a mídia instalação.
15. (Opcional) Ao terminar de usar a mídia de instalação, você poderá desanexar o volume. Depois de desanexar o volume, você poderá excluí-lo. Para obter mais informações, consulte [Desanexar um volume do Amazon EBS de uma instância Windows \(p. 1290\)](#) e [Excluir um volume de Amazon EBS \(p. 1293\)](#).

Adicionar componentes do Windows usando o Tools for Windows PowerShell

Use o seguinte procedimento para usar a Tools for Windows PowerShell para adicionar componentes do Windows à sua instância.

Para adicionar componentes do Windows à sua instância usando a Tools for Windows PowerShell

1. Use o cmdlet **Get-EC2Snapshot** com os filtros **Owner** e **description** para obter uma lista dos snapshots de mídia de instalação disponíveis.

```
PS C:\> Get-EC2Snapshot -Owner amazon -Filter @{ Name="description"; Values="Windows*" }
```
2. Na saída, observe o ID do snapshot que corresponde à arquitetura do sistema e seu idioma de preferência. Por exemplo:

```
...  
DataEncryptionKeyId :  
Description : Windows 2019 English Installation Media  
Encrypted : False  
KmsKeyId :  
OwnerAlias : amazon  
OwnerId : 123456789012  
Progress : 100%  
SnapshotId : snap-22da283e  
StartTime : 10/25/2019 8:00:47 PM  
State : completed  
StateMessage :  
Tags : {}  
VolumeId : vol-be5eafcb  
VolumeSize : 6  
...
```

3. Use o cmdlet [New-EC2Volume](#) para criar um volume do snapshot. Especifique a mesma zona de disponibilidade de sua instância.

```
PS C:\> New-EC2Volume -AvailabilityZone us-east-1a -VolumeType gp2 -  
SnapshotId snap-22da283e
```

4. Na saída, observe o ID do volume.

```
Attachments : {}  
AvailabilityZone : us-east-1a  
CreateTime : 4/18/2017 10:50:25 AM  
Encrypted : False  
Iops : 100  
KmsKeyId :  
Size : 6  
SnapshotId : snap-22da283e  
State : creating  
Tags : {}  
VolumeId : vol-06aa9e1fbf8b82ed1  
VolumeType : gp2
```

5. Use o cmdlet [Add-EC2Volume](#) para associar o volume à sua instância.

```
PS C:\> Add-EC2Volume -InstanceId i-087711ddaf98f9489 -VolumeId vol-06aa9e1fbf8b82ed1 -  
Device xvdh
```

6. Conecte-se à sua instância e disponibilize o volume. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#).

Important

Não inicialize o volume.

7. Abra o Painel de Controle, Programas e Recursos. Escolha Ativar ou desativar recursos do Windows. Se for solicitado pela mídia de instalação, especifique o volume do EBS com a mídia instalação.
8. (Opcional) Ao terminar de usar a mídia de instalação, use o cmdlet [Dismount-EC2Volume](#) para desanexar o volume da instância. Depois de desanexar o volume, você pode usar o cmdlet [Remove-EC2Volume](#) para excluir o volume.

Adicionar componentes do Windows usando a AWS CLI

Use o seguinte procedimento para usar o AWS CLI para adicionar componentes do Windows à sua instância.

Para adicionar componentes do Windows à sua instância usando a AWS CLI

1. Use o comando [describe-snapshots](#) com o parâmetro `owner-ids` e o filtro `description` para obter uma lista dos snapshots de mídia de instalação disponíveis.

```
aws ec2 describe-snapshots --owner-ids amazon --filters
    Name=description,Values=Windows*
```

2. Na saída, observe o ID do snapshot que corresponde à arquitetura do sistema e seu idioma de preferência. Por exemplo:

```
{
  "Snapshots": [
    ...
    {
      "OwnerAlias": "amazon",
      "Description": "Windows 2019 English Installation Media",
      "Encrypted": false,
      "VolumeId": "vol-be5eafcb",
      "State": "completed",
      "VolumeSize": 6,
      "Progress": "100%",
      "StartTime": "2019-10-25T20:00:47.000Z",
      "SnapshotId": "snap-22da283e",
      "OwnerId": "123456789012"
    },
    ...
  ]
}
```

3. Use o comando [create-volume](#) para criar um volume do snapshot. Especifique a mesma zona de disponibilidade de sua instância.

```
aws ec2 create-volume --snapshot-id snap-22da283e --volume-type gp2 --availability-
zone us-east-1a
```

4. Na saída, observe o ID do volume.

```
{
  "AvailabilityZone": "us-east-1a",
  "Encrypted": false,
  "VolumeType": "gp2",
  "VolumeId": "vol-0c98b37f30bcbe290",
  "State": "creating",
  "Iops": 100,
  "SnapshotId": "snap-22da283e",
  "CreateTime": "2017-04-18T10:33:10.940Z",
  "Size": 6
}
```

5. Use o comando [attach-volume](#) para associar o volume à sua instância.

```
aws ec2 attach-volume --volume-id vol-0c98b37f30bcbe290 --instance-
id i-01474ef662b89480 --device xvdg
```

6. Conecte-se à sua instância e disponibilize o volume. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#).

Important

Não initialize o volume.

7. Abra o Painel de Controle, Programas e Recursos. Escolha Ativar ou desativar recursos do Windows. Se for solicitado pela mídia de instalação, especifique o volume do EBS com a mídia instalação.
8. (Opcional) Ao terminar de usar a mídia de instalação, use o comando `detach-volume` para desanexar o volume da instância. Depois de desanexar o volume, você pode usar o comando `delete-volume` para excluir o volume.

Configurar um endereço IPv4 privado secundário para uma instância do Windows.

Você pode especificar vários endereços IPv4 privados para as instâncias. Depois de atribuir um endereço IPv4 privado secundário a uma instância, você precisa configurar o sistema operacional na instância para reconhecer o endereço IPv4 privado secundário.

Configurar o sistema operacional em uma instância do Windows para reconhecer um endereço IPv4 privado secundário requer o seguinte:

Tópicos

- [Etapas de pré-requisitos \(p. 610\)](#)
- [Etapa 1: Configurar o endereçamento IP estático na instância do Windows \(p. 610\)](#)
- [Etapa 2: Configurar um endereço IP privado secundário para a instância \(p. 612\)](#)
- [Etapa 3: Configurar as aplicações para usar o endereço IP privado secundário \(p. 613\)](#)

Note

Essas instruções são baseadas no Windows Server 2008 R2. A implantação dessas etapas pode variar dependendo do sistema operacional da instância do Windows.

Antes de começar

Como prática recomendada, execute suas instâncias do Windows usando as AMIs mais recentes. Se você estiver usando uma AMI em Windows mais antiga, assegure-se que tenha o hot fix Microsoft mencionado em <http://support.microsoft.com/kb/2582281>.

Etapas de pré-requisitos

1. Atribua o endereço IPv4 privado secundário à interface de rede para a instância. Você pode atribuir o endereço IPv4 privado secundário ao iniciar a instância ou após a instância estar em execução. Para obter mais informações, consulte [Atribuir um endereço IPv4 privado secundário \(p. 966\)](#).
2. Aloque um endereço de IP elástico ao endereço IPv4 privado secundário. Para obter mais informações, consulte [Alocar um endereço IP elástico \(p. 994\)](#) e [Associar um endereço IP elástico ao endereço IPv4 privado secundário \(p. 968\)](#).

Etapa 1: Configurar o endereçamento IP estático na instância do Windows

Para permitir que sua instância do Windows use vários endereços IP, configure sua instância para usar o endereçamento IP estático em vez de um servidor DHCP.

Important

Quando você configura o endereçamento IP estático na sua instância, o endereço IP deve corresponder exatamente o que é exibido no console, na CLI ou na API. Se você inserir esses endereços IP incorretamente, a instância poderia tornar-se inacessível.

Para configurar o endereçamento IP estático em uma instância do Windows

1. Conecte-se à sua instância.
2. Encontre o endereço IP, a máscara da sub-rede e os endereços gateway padrão para a instância ao executar as seguintes etapas:
 - Em uma janela do prompt de comando, execute o comando a seguir:

```
ipconfig /all
```

Revise a seção a seguir na sua saída e observe os valores de IPv4 Address (Endereço IPv4), Subnet Mask (Máscara de sub-rede), Default Gateway (Gateway padrão) e DNS Servers (Servidores DNS) da interface de rede.

```
Ethernet adapter Local Area Connection:
```

```
Connection-specific DNS Suffix . :  
Description . . . . . :  
Physical Address . . . . . :  
DHCP Enabled. . . . . :  
Autoconfiguration Enabled . . . . :  
IPv4 Address. . . . . : 10.0.0.131  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : 10.0.0.1  
DNS Servers . . . . . : 10.1.1.10  
10.1.1.20
```

3. Abra Central de Rede e Compartilhamento ao executar o comando a seguir:

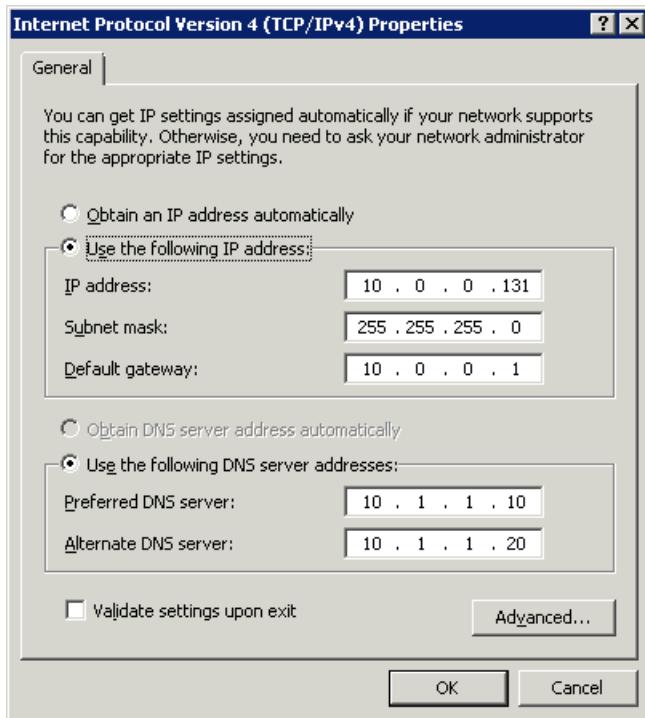
```
%SystemRoot%\system32\control.exe ncpa.cpl
```

4. Abra o menu contextual (botão direito do mouse) para interface de rede (Conexão Local) e selecione Propriedades.
5. Escolha Protocolo TCP/IP Versão 4 (TCP/IPv4), Propriedades.
6. Na caixa de diálogo Propriedades do Protocolo TCP/IP Versão 4 (TCP/IPv4), selecione Usar o seguinte endereço IP, insira os valores a seguir e escolha OK.

Campo	Valor
IP address	O endereço IPv4 obtido na etapa 2 acima.
Máscara de sub-rede	A máscara de sub-rede obtida na etapa 2 acima.
Gateway padrão	O endereço do gateway padrão obtido na etapa 2 acima.
Servidor DNS preferido	O servidor DNS obtido na etapa 2 acima.
Servidor DNS alternativo	O servidor DNS alternativo obtido na etapa 2 acima. Se um servidor DNS alternativo não estiver listado, deixe esse campo em branco.

Important

Se você definir o endereço IP para qualquer valor além do endereço IP atual, perderá conectividade com a instância.



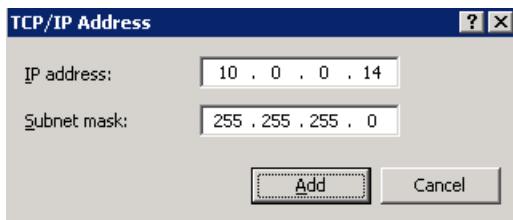
Você perderá conectividade do RDP com a instância do Windows por alguns segundos enquanto a instância converte entre uso de DHCP para endereçamento estático. A instância retém a mesma informação de endereços IP que antes, mas agora essa informação é estática e não é gerenciada por DHCP.

Etapa 2: Configurar um endereço IP privado secundário para a instância

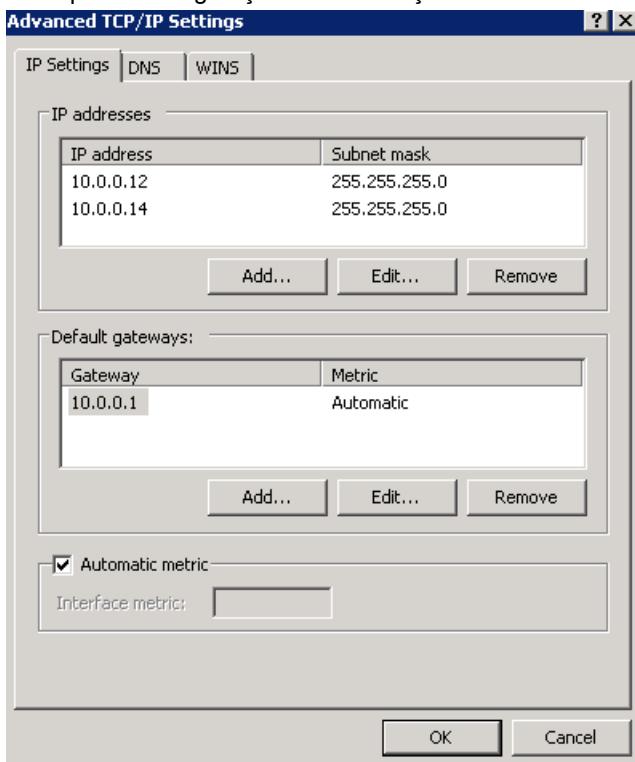
Depois de configurar o endereçamento IP estático na sua instância do Windows, você estará pronto para preparar um segundo endereço IP privado.

Como configurar um endereço IP secundário

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Na (Networking (Rede)), observe o endereço IP secundário.
4. Conecte-se à sua instância.
5. Na sua instância do Windows, selecione Iniciar, Painel de Controle.
6. Escolha Rede e Internet, Central de Rede e Compartilhamento.
7. Selecione a interface de rede (Conexão Local) e escolha Propriedades.
8. Na página Propriedades da Conexão Local, escolha Protocolo TCP/IP Versão 4 (TCP/IPv4), Propriedades, Avançado.
9. Escolha Adicionar.
10. Na caixa de diálogo Endereço TCP/IP, digite o endereço IP privado secundário para o endereço IP. Em Subnet mask (Máscara de sub-rede), digite a mesma máscara de sub-rede inserida para o endereço IP privado primário em [Etapa 1: Configurar o endereçamento IP estático na instância do Windows \(p. 610\)](#) e selecione Add (Adicionar).



11. Verifique as configurações de endereço IP e selecione OK.



12. Escolha OK, Fechar.
13. Para confirmar que o endereço IP secundário foi adicionado ao sistema operacional, em um prompt de comando, execute o comando ipconfig /all.

Etapa 3: Configurar as aplicações para usar o endereço IP privado secundário

Você pode configurar quaisquer aplicações para usar o endereço IP privado secundário. Por exemplo, se sua instância estiver executando um site no IIS, você pode configurar o IIS para usar o endereço IP privado secundário.

Para configurar o IIS para usar o endereço IP privado secundário

1. Conecte-se à sua instância.
2. Abra o Gerenciador do Serviços de Informações da Internet (IIS).
3. No painel Conexões, expanda Sites.
4. Abra o menu contextual (botão direito do mouse) para seu site ou selecione Editar Ligações.
5. Na caixa de diálogo Ligações do Site, para Tipo, escolha http, Editar.

6. Na caixa de diálogo Editar Ligação do Site, para Endereço IP, selecione o endereço IP privado secundário. (Por padrão, cada site aceita solicitações HTTP de todos os endereços IP.)



7. Escolha OK, Fechar.

Executar comandos na instância do Windows na inicialização

Ao executar uma instância do Windows no Amazon EC2, você pode passar os dados do usuário para a instância que pode ser usada para realizar tarefas de configuração automatizadas ou executar scripts após a inicialização da instância. Os dados do usuário da instância são tratados como dados opacos, cabe à instância interpretá-los. Os dados do usuário são processados pelo EC2Launch v2 ([AMIs de visualização compatíveis e por download \(p. 487\)](#)), pelo [EC2Launch \(p. 522\)](#) no Windows Server 2016 e versões posteriores e pelo [EC2Config \(p. 530\)](#) no Windows Server 2012 R2 e versões anteriores.

Para obter exemplos de assembly de uma propriedade `UserData` em um modelo do AWS CloudFormation, consulte [Propriedade UserData codificada em Base64](#) e [Propriedade UserData codificada em Base64 com AccessKey e SecretKey](#).

Para obter informações sobre a execução de comandos na instância do Linux na inicialização, consulte [Executar comandos na instância do Linux na inicialização](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

- [Scripts de dados do usuário \(p. 614\)](#)
- [Execução de dados do usuário \(p. 616\)](#)
- [Dados do usuário e console \(p. 619\)](#)
- [Dados do usuário e Tools for Windows PowerShell \(p. 620\)](#)

Scripts de dados do usuário

Para que o EC2Config ou o EC2Launch execute scripts, será necessário colocar o script em uma tag especial ao adicioná-lo aos dados do usuário. A tag usada depende de os comandos serem executados em uma janela de prompt de comando (comandos de lote) ou usando o Windows PowerShell.

Se você especificar um script em lote e um script do Windows PowerShell, o script em lote é executado primeiro e o script do Windows PowerShell é executado em seguida, independentemente da ordem em que eles aparecem nos dados do usuário da instância.

Se você usar uma API da AWS, incluindo a AWS CLI, em um script de dados de usuário, deverá usar um perfil de instância ao inicializar a instância. Um perfil de instância fornece as credenciais apropriadas

da AWS exigidas pelo script de dados do usuário para executar a chamada de API. Para obter mais informações, consulte [Perfis de instância \(p. 1196\)](#). As permissões que atribui à função do IAM dependem de quais serviços você chama com a API. Para obter mais informações, consulte [Funções do IAM para Amazon EC2](#).

Tipo de script

- [Sintaxe para scripts em lote \(p. 615\)](#)
- [Sintaxe para scripts do Windows PowerShell \(p. 615\)](#)
- [Sintaxe para scripts de configuração YAML \(p. 616\)](#)
- [Codificação base64 \(p. 616\)](#)

Sintaxe para scripts em lote

Especifique um script em lote usando a tag `script`. Separe os comandos usando quebras de linha. Por exemplo:

```
<script>
echo Current date and time >> %SystemRoot%\Temp\test.log
echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
```

Por padrão, os scripts de dados do usuário são executados uma vez ao inicializar a instância. Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>` aos dados do usuário.

```
<script>
echo Current date and time >> %SystemRoot%\Temp\test.log
echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
</script>
<persist>true</persist>
```

Sintaxe para scripts do Windows PowerShell

As AMIs do Windows da AWS incluem o [AWS Tools for Windows PowerShell](#) para que você possa especificar esses cmdlets nos dados do usuário. Se você associar uma função do IAM à sua instância, não será necessário especificar as credenciais para os cmdlets, pois os aplicativos em execução na instância usam as credenciais da função para acessar os recursos da AWS (por exemplo, buckets do Amazon S3).

Especifique um script do Windows PowerShell usando a tag `powershell`. Separe os comandos usando quebras de linha. Por exemplo:

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
```

Por padrão, os scripts de dados do usuário são executados uma vez ao inicializar a instância. Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>` aos dados do usuário.

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
```

```
<persist>true</persist>
```

Sintaxe para scripts de configuração YAML

Se você estiver usando o EC2Launch v2 para executar scripts, poderá usar o formato YAML. Para visualizar tarefas de configuração, detalhes e exemplos do EC2Launch v2, consulte [Configuração de tarefas do EC2Launch v2 \(p. 503\)](#).

Especifique um script YAML com a tarefa `executeScript`.

Exemplo de sintaxe do YAML para executar um script do PowerShell

```
version: 1.0
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
  content: |-
    $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
    New-Item $file -ItemType file
```

Exemplo de sintaxe do YAML para executar um script em lote

```
version: 1.0
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: batch
    runAs: localSystem
  content: |-
    echo Current date and time >> %SystemRoot%\Temp\test.log
    echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Codificação base64

Se você estiver usando a API do Amazon EC2 ou uma ferramenta que não execute codificação base64 dos dados do usuário, codifique você mesmo os dados do usuário. Caso contrário, será registrado um erro sobre não ser possível encontrar as tags `script` ou `powershell` para executar. A seguir está um exemplo que codifica usando o Windows PowerShell.

```
$UserData =
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

A seguir está um exemplo que decodifica usando o PowerShell.

```
$Script =
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Para obter mais informações sobre a codificação base64, consulte <https://www.ietf.org/rfc/rfc4648.txt>.

Execução de dados do usuário

Por padrão, todas as AMIs do Windows da AWS têm a execução de dados de usuário habilitada para a execução inicial. É possível especificar que os scripts de dados do usuário sejam executados na próxima

vez que a instância for reiniciada. Também é possível especificar que os scripts de dados do usuário sejam executados toda vez que a instância for reiniciada.

Os scripts de dados do usuário são executados na conta do administrador local quando uma senha aleatória é gerada. Caso contrário, os scripts de dados do usuário são executados na conta do sistema.

Execução da instância

Os scripts nos dados do usuário da instância são executados durante a execução inicial da instância. Se a tag `persist` for localizada, a execução de dados do usuário será habilitada para reinicializações ou inicializações subsequentes. Os arquivos de log do EC2Launch v2, EC2Launch e EC2Config contêm a saída da saída padrão e dos fluxos de erro padrão.

EC2Launch v2

O arquivo de log para EC2Launch v2 é `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

Note

A pasta `C:\ProgramData` pode estar oculta. Para exibir a pasta, você deve mostrar arquivos e pastas ocultos.

As informações a seguir são registradas quando os dados do usuário são executados.

- `Info: Converting user-data to yaml format:` se os dados do usuário tiverem sido fornecidos no formato XML
- `Info: Initializing user-data state:` o início da execução de dados do usuário
- `Info: Frequency is: always:` se a tarefa de dados do usuário estiver sendo executada em cada inicialização
- `Info: Frequency is: once:` se a tarefa de dados do usuário estiver sendo executada apenas uma vez
- `Stage: postReadyUserData execution completed:` o final da execução de dados do usuário

EC2Launch

O arquivo de log do EC2Launch é `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\userdataExecution.log`.

A pasta `C:\ProgramData` pode estar oculta. Para exibir a pasta, você deve mostrar arquivos e pastas ocultos.

As informações a seguir são registradas quando os dados do usuário são executados.

- `Userdata execution begins:` o início da execução de dados do usuário
- `<persist> tag was provided: true:` se a tag `persist` for encontrada
- `Running userdata on every boot:` se a tag `persist` for encontrada
- `<powershell> tag was provided.. running powershell content:` se a tag `powershell` for encontrada
- `<script> tag was provided.. running script content:` se a tag de script for encontrada
- `Message: The output from user scripts:` se os scripts de dados do usuário forem executados, a saída será registrada

EC2Config

O arquivo de log do EC2Config é C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log. As informações a seguir são registradas quando os dados do usuário são executados.

- Ec2HandleUserData: Message: Start running user scripts: o início da execução de dados do usuário
- Ec2HandleUserData: Message: Re-enabled userdata execution: se a tag persist for encontrada
- Ec2HandleUserData: Message: Could not find <persist> and </persist>: se a tag persist não for encontrada
- Ec2HandleUserData: Message: The output from user scripts: se os scripts de dados do usuário forem executados, a saída será registrada

Reinicializações ou inicializações subsequentes

Quando você atualiza os dados do usuário da instância, os scripts de dados do usuário não são executados automaticamente ao reiniciar ou iniciar a instância. No entanto, você pode habilitar a execução de dados do usuário para que eles sejam executados uma vez ao reiniciar ou iniciar a instância, ou sempre que reiniciar ou iniciar a instância.

Se você escolher a opção Shutdown with Sysprep (Desativar com Sysprep), os scripts de dados do usuário serão executados na próxima vez que a instância for reiniciada ou iniciada, mesmo que você não tenha habilitado a execução de dados do usuário para reinicializações ou inicializações subsequentes. Os scripts de dados do usuário não serão executados em reinicializações ou inicializações subsequentes.

Como habilitar a execução de dados do usuário com o EC2Launch v2 (Visualizar AMIs)

- Para executar uma tarefa nos dados do usuário na primeira inicialização, defina frequency como once.
- Para executar uma tarefa nos dados do usuário em cada inicialização, defina frequency como always.

Como habilitar a execução de dados do usuário com o EC2Launch (Windows Server 2016 ou versões posteriores)

1. Conecte-se à sua instância do Windows.
2. Abra uma janela de comando do PowerShell e execute o comando a seguir:

```
C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
```

3. Desconecte-se da instância do Windows. Para executar scripts atualizados na próxima vez que a instância for iniciada, interrompa a instância e atualize os dados do usuário. Para obter mais informações, consulte [Visualizar e atualizar os dados do usuário da instância \(p. 619\)](#).

Como habilitar a execução de dados do usuário com EC2Config (Windows Server 2012 R2 e versões anteriores)

1. Conecte-se à sua instância do Windows.
2. Aberto C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe.
3. Em User Data (Dados do usuário), selecione Enable UserData execution for next service start (Habilitar execução de dados do usuário para o próximo início de serviço).
4. Desconecte-se da instância do Windows. Para executar scripts atualizados na próxima vez que a instância for iniciada, interrompa a instância e atualize os dados do usuário. Para obter mais informações, consulte [Visualizar e atualizar os dados do usuário da instância \(p. 619\)](#).

Dados do usuário e console

Você pode especificar os dados do usuário da instância ao executar uma instância. Se o volume raiz da instância for um volume do EBS, também é possível parar a instância e atualizar os dados de usuário.

Especificar os dados do usuário da instância na inicialização

Ao executar uma instância, especifique o script em Advanced Details (Detalhes avançados), User data (Dados do usuário), na página Step 3: Configure Instance Details (Etapa 3: configurar detalhes da instância) do assistente de execução de instância. O exemplo na seguinte imagem cria um arquivo na pasta temporária do Windows, usando a data e a hora atuais no nome de arquivo. Ao incluir <persist>true</persist>, o script é executado sempre que você reiniciar ou iniciar a instância. Ao selecionar As text (Como texto), o console do Amazon EC2 executa a codificação base64 para você.

The screenshot shows the 'Advanced Details' configuration page for a Windows instance. The 'User data' tab is selected. There are three radio button options: 'As text' (selected), 'As file', and 'Input'. Below the tabs is a text area containing a PowerShell script:

```
<powershell>
$file = $env:SystemRoot+
New-Item $file -ItemType fi
</powershell>
<persist>true</persist>
```

Visualizar e atualizar os dados do usuário da instância

Você pode visualizar dados do usuário da instância para qualquer instância e atualizar dados do usuário da instância para uma instância interrompida.

Para atualizar os dados do usuário para uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Instance state (Estado da instância) e Stop instance (Interromper instância).

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

4. Quando a confirmação for solicitada, escolha Parar. Pode demorar alguns minutos para que a instância pare.
5. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Edit user data (Editar dados de usuário). Não é possível alterar os dados do usuário se a instância estiver em execução, mas é possível visualizá-la.
6. Na caixa de diálogo Edit user data (Editar dados do usuário), atualize os dados do usuário e escolha Save (Salvar). Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione <persist>true</persist>, como mostrado no exemplo a seguir:

View/Change User Data

Instance ID: i-08240c2f0f225277a

User Data:

```
<powershell>
$file = $env:SystemRoot+"\Temp\"+(Get-Date).ToString("MM-d
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Plain text Input is already base64 encoded

7. Inicie a instância. Se você habilitou a execução de dados do usuário para reinicializações ou inicializações subsequentes, os scripts de dados do usuário atualizados serão executados como parte do processo de inicialização da instância.

Dados do usuário e Tools for Windows PowerShell

Você pode usar Tools for Windows PowerShell para especificar, modificar e ver os dados do usuário para sua instância. Para obter informações sobre como visualizar os dados do usuário da sua instância usando metadados de instância, consulte [Recuperar os dados do usuário da instância \(p. 639\)](#). Para obter informações sobre dados do usuário e a AWS CLI, consulte [User data and the AWS CLI \(Dados do usuário e a AWS CLI\)](#) no Amazon EC2 User Guide for Linux Instances (Manual do usuário do Amazon EC2 para instâncias do Linux).

Exemplo: especifique os dados do usuário da instância na inicialização

Crie um arquivo de texto com dados do usuário da instância. Para executar os scripts de dados do usuário sempre que você reiniciar ou iniciar a instância, adicione `<persist>true</persist>`, como mostrado no exemplo a seguir:

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Para especificar dados do usuário da instância ao executar a instância, use o comando [New-EC2Instance](#). Esse comando não executa a codificação base64 dos dados do usuário para você. Use os comandos a seguir para codificar os dados do usuário em um arquivo de texto denominado `script.txt`.

```
PS C:\> $Script = Get-Content -Raw script.txt
PS C:\> $UserData =
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Use o parâmetro `-UserData` para passar os dados do usuário para o comando [New-EC2Instance](#).

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
-KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
-UserData $UserData
```

Exemplo: atualizar dados do usuário da instância para uma instância interrompida

Você pode modificar os dados do usuário de uma instância interrompida usando o comando [Edit-EC2InstanceAttribute](#).

Crie um arquivo de texto com o novo script. Use os comandos a seguir para codificar os dados do usuário no arquivo de texto denominado `new-script.txt`.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
PS C:\> $NewUserData =
[System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Use os parâmetros `-UserData` e `-Value` para especificar os dados do usuário.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Exemplo: visualizar dados do usuário da instância

Para recuperar os dados do usuário para uma instância, use o comando [Get-EC2InstanceAttribute](#).

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
userData).UserData
```

A seguir está um exemplo de saída. Observe que os dados do usuário são codificados.

```
PHBvd2Vyc2h1bGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlcilkyXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Use os comandos a seguir para armazenar os dados de usuário codificados em uma variável e decodifique-os.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded))
```

A seguir está um exemplo de saída.

```
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
```

```
</powershell>
<persist>true</persist>
```

Exemplo: renomear a instância para corresponder ao valor da tag

Para ler o valor da tag, renomeie a instância na primeira inicialização para corresponder ao valor da tag e reinicialize. Use o comando [Get-EC2Tag](#). Para executar esse comando com êxito, é necessário ter uma função com permissões ec2:DescribeTags, pois as informações de tag não estão disponíveis nos metadados e devem ser recuperadas pela chamada de API. Para obter mais informações sobre como anexar uma função a uma instância, consulte [Anexar uma função do IAM a uma instância](#).

Note

Esse script falha em versões do Windows Server anteriores a 2008.

```
<powershell>
$instanceId = (invoke-webrequest http://169.254.169.254/latest/meta-data/instance-id - 
UseBasicParsing).content
$nameValue = (get-ec2tag -filter @{Name="resource-id";Value=
$instanceid},{@{Name="key";Value="Name"}}).Value
$pattern = "^(?!([0-9]{1,15})[a-zA-Z0-9-]{1,15}$"
##Verify Name Value satisfies best practices for Windows hostnames
If ($nameValue -match $pattern)
{
    Try
        {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
    Catch
        {$_Exception.Message
        Write-Output "Rename failed: $_Exception.Message"}
}
Else
{
    Throw "Provided name not a valid hostname. Please ensure Name value is between 1 and
15 characters in length and contains only alphanumeric or hyphen characters"
}
</powershell>
```

Metadados da instância e dados do usuário

Os metadados da instância são dados sobre sua instância que você pode usar para configurar ou gerenciar a instância em execução. Os metadados de instância são divididos em [categorias \(p. 640\)](#), por exemplo, nome do host, eventos e grupos de segurança.

Você também pode usar os metadados da instância para acessar os dados do usuário que você especificou ao executar sua instância. Por exemplo, é possível especificar parâmetros para configurar a instância ou incluir um script simples. É possível criar AMIs genéricas e usar dados do usuário para modificar os arquivos de configuração fornecidos na hora da inicialização. Por exemplo, se você executar servidores Web para várias empresas de pequeno porte, elas poderão usar a mesma AMI genérica e recuperar o conteúdo do bucket do Amazon S3 que você especifica nos dados do usuário na inicialização. Para adicionar um novo cliente a qualquer momento, crie um bucket para o cliente, adicione seu conteúdo e inicie a AMI com o nome exclusivo do bucket fornecido ao código nos dados do usuário. Se você executar mais de uma instância ao mesmo tempo, os dados do usuário estarão disponíveis para todas as instâncias nessa reserva. Cada instância que faz parte da mesma reserva tem um número de ami-launch-index exclusivo que permite escrever código que controla o que fazer. Por exemplo, o primeiro host pode se eleger como o nó original em um cluster.

As instâncias do EC2 também podem incluir dados dinâmicos, como um documento de identidade de instância que é gerado quando a instância é executada. Para obter mais informações, consulte [Categorias de dados dinâmicos \(p. 648\)](#).

Important

Embora você só possa acessar os metadados de instância e os dados do usuário de dentro da própria instância, os dados não são protegidos por autenticação ou métodos de criptografia.

Qualquer usuário que tenha acesso direto à instância e, potencialmente, qualquer software em execução na instância, pode visualizar seus metadados. Portanto, você não deve armazenar dados confidenciais, como senhas ou chaves de criptografia de longa duração, como dados de usuário.

Note

Os exemplos nesta seção usam o endereço IPv4 do serviço de metadados da instância: 169.254.169.254. Se você estiver recuperando metadados de instância para instâncias do EC2 sobre o endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: fd00:ec2::254. O endereço IPv6 do serviço de metadados da instância é compatível com comandos IMDSv2. O endereço IPv6 só é acessível no [Instâncias criadas no Sistema Nitro \(p. 154\)](#).

Tópicos

- [Usar IMDSv2 \(p. 623\)](#)
- [Configurar as opções de metadados da instância \(p. 627\)](#)
- [Recuperar metadados da instância \(p. 630\)](#)
- [Trabalhar com dados do usuário da instância \(p. 638\)](#)
- [Recuperar dados dinâmicos \(p. 640\)](#)
- [Categorias de metadados da instância \(p. 640\)](#)
- [Documentos de identidade da instância \(p. 648\)](#)

Usar IMDSv2

É possível acessar metadados de instância em uma instância em execução usando um dos seguintes métodos:

- Serviço de metadados da instância versão 1 (IMDSv1) – um método de solicitação/resposta
- Serviço de metadados da instância versão 2 (IMDSv2) – um método orientado a sessões

Por padrão, você pode usar o IMDSv1 ou o IMDSv2 ou ambos. O serviço de metadados da instância faz distinção entre as solicitações do IMDSv1 e do IMDSv2 com base na presença dos cabeçalhos de `PUT` ou de `GET`, que são exclusivos do IMDSv2, em qualquer solicitação. Para obter mais informações, consulte [Adicionar defesa profunda contra firewalls abertos, proxies reversos e vulnerabilidades SSRF com melhorias no serviço de metadados da instância do EC2](#).

Você pode configurar o serviço de metadados da instância em cada instância de forma que o código ou os usuários locais usem o IMDSv2. Quando você especifica que o IMDSv2 deve ser usado, o IMDSv1 não funciona mais. Para obter mais informações, consulte [Configurar as opções de metadados da instância \(p. 627\)](#).

Para recuperar metadados da instância, consulte [Recuperar metadados da instância \(p. 630\)](#).

Note

Os exemplos nesta seção usam o endereço IPv4 do serviço de metadados da instância: 169.254.169.254. Se você estiver recuperando metadados de instância para instâncias do EC2 sobre o endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: fd00:ec2::254. O endereço IPv6 do serviço de metadados da instância é compatível com comandos IMDSv2. O endereço IPv6 só é acessível no [Instâncias criadas no Sistema Nitro \(p. 154\)](#).

Como Serviço de metadados da instância versão 2 funciona

O IMDSv2 usa solicitações orientadas a sessão. Com solicitações orientadas a sessão, você cria um token de sessão que define a duração da sessão, que pode ser, no mínimo, um segundo e, no máximo,

seis horas. Durante o período especificado, você pode usar o mesmo token de sessão para solicitações subsequentes. Depois que a duração especificada expira, você deve criar um novo token de sessão para uso em solicitações futuras.

O exemplo a seguir usa um script shell do PowerShell e o IMDSv2 para recuperar os itens de metadados de nível superior de instância. O exemplo:

- Cria um token de sessão que dura seis horas (21.600 segundos) usando a solicitação `PUT`.
- Armazena o cabeçalho do token da sessão em uma variável chamada `token`
- Solicita os itens de metadados de nível superior usando o token

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{$"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/
```

Depois de criar um token, você pode reutilizá-lo até que ele expire. No comando de exemplo a seguir, que obtém o ID da AMI usada para executar a instância, o token armazenado em `$token` no exemplo anterior é reutilizado.

```
PS C:\> Invoke-RestMethod -Headers @{$"X-aws-ec2-metadata-token" = $token} -Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Quando você usa o IMDSv2 para solicitar os metadados da instância, a solicitação deve incluir o seguinte:

1. Use uma solicitação `PUT` para solicitar a inicialização de uma sessão para o serviço de metadados da instância. A solicitação `PUT` retorna um token que deve ser incluído em solicitações `GET` subsequentes para o serviço de metadados da instância. O token é exigido para acessar metadados usando o IMDSv2.
2. Inclua o token em todas as solicitações `GET` para o serviço de metadados da instância. Quando o uso do token está definido como `required`, as solicitações sem um token válido ou com um token expirado recebem um código de erro HTTP 401 – `Unauthorized`. Para obter informações sobre como alterar o uso do token, consulte [modify-instance-metadata-options](#) na AWS CLI Command Reference (Referência de comandos da AWS CLI).
 - O token é uma chave específica da instância. O token não é válido em outras instâncias do EC2 e será rejeitado se você tentar usá-lo fora da instância na qual foi gerado.
 - A solicitação `PUT` deve incluir um cabeçalho que especifique a vida útil (TTL) do token, em segundos, até um máximo de seis horas (21.600 segundos). O token representa uma sessão lógica. O TTL especifica o período de validade do token e, portanto, a duração da sessão.
 - Depois que o token expira, para continuar a acessar os metadados da instância, você deve criar uma nova sessão usando outro `PUT`.
 - É possível optar por reutilizar um token ou criar um novo token para cada solicitação. Para um número pequeno de solicitações, pode ser mais fácil gerar e usar imediatamente um token a cada vez que você precisar acessar o serviço de metadados da instância. Mas, para obter eficiência, você pode especificar uma duração maior para o token e reutilizá-lo, em vez de precisar escrever uma solicitação `PUT` toda vez que precisar solicitar metadados da instância. Não há um limite prático para o número de tokens simultâneos, cada um representando sua própria sessão. No entanto, o IMDSv2 ainda é restrinido pela conexão do serviço de metadados da instância e pelos limites de controle de utilização. Para obter mais informações, consulte [Limitação de consulta \(p. 636\)](#).

Os métodos HTTP `GET` e `HEAD` são permitidos em solicitações de metadados de instâncias do IMDSv2. As solicitações `PUT` serão rejeitadas se contiverem um cabeçalho `X-Forwarded-For`.

Por padrão, a resposta a solicitações PUT tem um limite de saltos de resposta (vida útil) de 1 no nível de protocolo IP. É possível ajustar o limite de saltos usando o comando `modify-instance-metadata-options` se você precisar de um limite maior. Por exemplo, um limite de saltos maior pode ser necessário para compatibilidade com versões anteriores de serviços de contêiner em execução na instância. Para obter mais informações, consulte [modify-instance-metadata-options](#) na AWS CLI Command Reference (Referência de comandos da AWS CLI).

Transição para usar o Serviço de metadados da instância versão 2

O uso do Serviço de metadados de instância versão 2 (IMDSv2) é opcional. O Serviço de metadados de instância versão 1 (IMDSv1) continuará a ter suporte indefinidamente. Se você optar por migrar usando o IMDSv2, recomendamos usar as ferramentas e o caminho de transição a seguir.

Ferramentas para ajudar com a transição para o IMDSv2

Se seu software usar o IMDSv1, use as ferramentas a seguir para ajudar a configurar o software para usar o IMDSv2.

- Software da AWS: as versões mais recentes dos AWS SDKs e CLIs oferecem suporte ao IMDSv2. Para usar o IMDSv2, verifique se as instâncias do EC2 têm as versões mais recentes dos AWS SDKs e CLIs. Para obter informações sobre como atualizar a CLI, consulte [Installing, updating, and uninstalling the AWS CLI \(Instalar, atualizar e desinstalar a AWS CLI\)](#) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).
- CloudWatch: o IMDSv2 usa sessões com token, enquanto o IMDSv1 não. A métrica `MetadataNoToken` do CloudWatch rastreia o número de chamadas para o serviço de metadados da instância que estão usando o IMDSv1. Rastreando essa métrica até zero, você pode determinar se e quando todo o software foi atualizado para usar o IMDSv2. Para obter mais informações, consulte [Métricas de instância \(p. 902\)](#).
- Atualizações das CLIs e APIs do EC2: para instâncias existentes, é possível usar o comando `modify-instance-metadata-options` da CLI (ou a API `ModifyInstanceMetadataOptions`) para exigir o uso do IMDSv2. Para novas instâncias, é possível usar o comando `run-instances` da CLI (ou a API `RunInstances`) e o parâmetro `metadata-options` para executar novas instâncias que exigem o uso do IMDSv2.

Para exigir o uso do IMDSv2 em todas as novas instâncias executadas por grupos de Auto Scaling, seus grupos de Auto Scaling podem usar um modelo de execução ou uma configuração de execução. Quando você [cria um modelo de execução](#) ou [cria uma configuração de execução](#), você deve configurar os parâmetros de `MetadataOptions` para exigir o uso do IMDSv2. Depois que você configura o modelo de execução ou a configuração de execução, o grupo de Auto Scaling executa novas instâncias usando o novo modelo de execução ou configuração de execução, mas as instâncias existentes não são afetadas.

Use o comando `modify-instance-metadata-options` da CLI (ou a API `ModifyInstanceMetadataOptions`) para exigir o uso do IMDSv2 em instâncias existentes, ou encerre as instâncias e o grupo de Auto Scaling executará novas instâncias de substituição com as configurações das opções de metadados de instância definidas no modelo ou na configuração de execução.

- Políticas do IAM e SCPs: é possível usar uma condição do IAM para exigir que os usuários do IAM não executem uma instância a menos que ela use IMDSv2. Também é possível usar condições do IAM para exigir que os usuários do IAM não podem executar instâncias para habilitar novamente o IMDSv1 e exigir que o serviço de metadados da instância esteja disponível na instância.

As chaves de condição `ec2:MetadataHttpTokens`, `ec2:MetadataHttpPutResponseHopLimit` e `ec2:MetadataHttpEndpoint` do IAM podem ser usadas para controlar o uso de `RunInstances` e da API `ModifyInstanceMetadataOptions` e CLI correspondente. Se uma política for criada, e um parâmetro na chamada à API não corresponder ao estado especificado na política usando a chave de condição, a chamada à API ou à CLI falhará com uma resposta `UnauthorizedOperation`. Essas chaves de condição podem ser usadas em políticas do IAM ou políticas de controle de serviço (SCPs) do AWS Organizations.

Além disso, é possível escolher uma camada adicional de proteção para exigir a alteração do IMDSv1 para o IMDSv2. Na camada de gerenciamento de acesso com relação às APIs chamadas por meio de credenciais de função do EC2, você pode usar uma nova chave de condição nas políticas do IAM ou nas políticas de controle de serviço (SCPs) do AWS Organizations. Especificamente, ao usar a chave da condição da política `ec2:RoleDelivery` com um valor de `2.0` nas políticas do IAM, as chamadas à API feitas com credenciais de função do EC2 obtidas do IMDSv1 receberão uma resposta `UnauthorizedOperation`. A mesma coisa pode ser obtida de forma mais ampla com essa condição exigida por uma SCP. Isso garante que as credenciadas entregues por meio do IMDSv1 não podem ser realmente usadas para chamar APIs porque todas as chamadas à API que não corresponderem à condição especificada receberão um erro `UnauthorizedOperation`. Para obter exemplos de políticas do IAM, consulte [Trabalhar com metadados de instância \(p. 1182\)](#). Para obter mais informações, consulte [Políticas de controle de serviço](#) no Guia do usuário do AWS Organizations.

Caminho recomendado para exigir acesso ao IMDSv

Usando as ferramentas acima, recomendamos que você siga este caminho para fazer a transição para o IMDSv2:

[Etapa 1: No início](#)

Atualize os SDKs, as CLIs e o software que usam credenciais de função em suas instâncias do EC2 para versões compatíveis com o IMDSv2. Para obter informações sobre como atualizar a CLI, consulte [Upgrading to the latest version of the AWS CLI \(Fazer upgrade para a versão mais recente da AWS CLI\)](#) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).

Depois, altere o software que acessa os metadados da instância diretamente (ou seja, que não usa um SDK) usando as solicitações do IMDSv2.

[Etapa 2: Durante a transição](#)

Acompanhe o andamento da transição usando a métrica do CloudWatch `MetadataNoToken`. Essa métrica mostra o número de chamadas para o serviço de metadados da instância que estão usando o IMDSv1 em suas instâncias. Para obter mais informações, consulte [Métricas de instância \(p. 902\)](#).

[Etapa 3: Quando tudo estiver pronto em todas as instâncias](#)

Tudo estará pronto em todas as instâncias quando a métrica do CloudWatch `MetadataNoToken` registrar uso zero do IMDSv1. Nessa fase, é possível fazer o seguinte:

- Nessa fase, você pode exigir o uso do IMDSv2 por meio do comando `modify-instance-metadata-options`. É possível fazer essas alterações em instâncias em execução. Não é necessário reiniciar as instâncias.
- Para novas instâncias: ao executar uma nova instância, é possível seguir um destes procedimentos:
 - No assistente de instância de execução do console do Amazon EC2, defina `Metadata accessible` (Metadados acessíveis) como `Enabled` (Habilitado) e `Metadata version` (Versão de metadados) como `V2`. Para obter mais informações, consulte [Etapa 3: configurar detalhes da instância \(p. 421\)](#).
 - Use o comando `run-instances` para especificar que apenas o IMDSv2 deve ser usado.

A atualização de opções de metadados de instâncias existentes está disponível apenas por meio da API ou AWS CLI. No momento, não está disponível no console do Amazon EC2. Para obter mais informações, consulte [Configurar as opções de metadados da instância \(p. 627\)](#).

[Etapa 4: Quando todas as suas instâncias tiverem feito a transição para o IMDSv2](#)

As chaves de condição `ec2:MetadataHttpTokens`, `ec2:MetadataHttpPutResponseHopLimit` e `ec2:MetadataHttpEndpoint` do IAM podem ser usadas para controlar o uso de `RunInstances` e da API `ModifyInstanceMetadataOptions` e CLI correspondente. Se uma política for criada, e um parâmetro

na chamada à API não corresponder ao estado especificado na política usando a chave de condição, a chamada à API ou à CLI falhará com uma resposta `UnauthorizedOperation`. Para obter exemplos de políticas do IAM, consulte [Trabalhar com metadados de instância \(p. 1182\)](#).

Configurar as opções de metadados da instância

As opções de metadados de instância permitem configurar instâncias novas ou existentes para fazer o seguinte:

- Exigir o uso do IMDSv2 ao solicitar metadados de instância
- Especificar o limite de salto de resposta `PUT`
- Desativar o acesso aos metadados da instância

Também é possível usar chaves de condição do IAM em uma política do IAM ou SCP para fazer o seguinte:

- Permitir que uma instância seja executada somente se ela estiver configurada para exigir o uso do IMDSv2
- Restringir o número de saltos permitidos
- Desativar o acesso aos metadados da instância

Note

Se a versão do PowerShell for anterior à 4.0, [atualize para o Windows Management Framework 4.0](#) para exigir o uso do IMDSv2.

Note

Proceda com cautela e conduza testes cuidadosos antes de fazer qualquer alteração. Anote o seguinte:

- Se você exigir o uso do IMDSv2, as aplicações ou agentes que usam o IMDSv1 para acesso aos metadados da instância falharão.
- Se você desativar todo o acesso aos metadados da instância, as aplicações ou agentes que contam com o acesso aos metadados da instância para funcionarem falharão.
- Para IMDSv2, você deve usar o token `/latest/api/` ao recuperar o token.

Tópicos

- [Configurar opções de metadados da instância para novas instâncias \(p. 627\)](#)
- [Modificar as opções de metadados de instância para as instâncias existentes \(p. 629\)](#)

Configurar opções de metadados da instância para novas instâncias

É possível exigir o uso do IMDSv2 em uma instância ao executá-la. Você também pode criar uma política do IAM que impeça que os usuários executem novas instâncias, a menos que exijam o IMDSv2 na nova instância.

Console

Como exigir o uso do IMDSv2 em uma nova instância

- Ao executar uma nova instância no console do Amazon EC2, selecione as seguintes opções na página `Configure Instance Details` (Configurar detalhes da instância):

- Em Advanced Details (Detalhes avançados), em Metadata accessible (Metadados acessíveis), selecione Enabled (Habilitado).
- Em Metadata version (Versão de metadados), selecione V2 (token required) V2 (token obrigatório).

Para obter mais informações, consulte [Etapa 3: configurar detalhes da instância \(p. 421\)](#).

AWS CLI

Como exigir o uso do IMDSv2 em uma nova instância

O exemplo de `run-instances` a seguir executa uma instância `c3.large` com `--metadata-options` definido como `HttpTokens=required`. Quando você especifica um valor para `HttpTokens`, você também deve definir `HttpEndpoint` como `enabled`. Como o cabeçalho de token seguro é definido como `required` para solicitações de recuperação de metadados, ele opta por exigir o uso do IMDSv2 na instância ao solicitar metadados da instância.

```
aws ec2 run-instances
  --image-id ami-0abcdef1234567890
  --instance-type c3.large
  ...
  --metadata-options "HttpEndpoint=enabled,HttpTokens=required"
```

Como exigir o uso do IMDSv2 em todas as novas instâncias

Para garantir que os usuários do IAM podem executar apenas instâncias que usam o IMDSv2 ao solicitar metadados da instância, você pode especificar que a condição para exigir o IMDSv2 deve ser atendida para que uma instância possa ser executada. Para ver um exemplo de política do IAM, consulte [Trabalhar com metadados de instância \(p. 1182\)](#).

Console

Como desabilitar o acesso aos metadados da instância

- Para garantir que o acesso aos metadados da instância esteja desativado, independentemente da versão do serviço de metadados da instância que você esteja usando, inicie a instância no console do Amazon EC2 com a seguinte opção selecionada na página `Configure Instance Details` (Configurar os detalhes da instância):
 - Em Advanced Details (Detalhes avançados), em Metadata accessible (Metadados acessíveis), selecione `Disabled` (Desabilitado).

Para obter mais informações, consulte [Etapa 3: configurar detalhes da instância \(p. 421\)](#).

AWS CLI

Como desabilitar o acesso aos metadados da instância

Para garantir que o acesso aos metadados da instância esteja desativado, independentemente da versão do serviço de metadados da instância que você esteja usando, inicie a instância com `--metadata-options` definido como `HttpEndpoint=disabled`. Você pode habilitar o acesso posteriormente usando o comando `modify-instance-metadata-options`.

```
aws ec2 run-instances
  --image-id ami-0abcdef1234567890
  --instance-type c3.large
  ...
```

```
--metadata-options "HttpEndpoint=disabled"
```

Modificar as opções de metadados de instância para as instâncias existentes

É possível exigir o uso do IMDSv2 em uma instância existente. Você também pode alterar o limite de saltos de resposta PUT e desativar o acesso aos metadados em uma instância existente. Também é possível criar uma política do IAM que impeça que os usuários modifiquem as opções de metadados em uma instância existente.

Atualmente apenas o AWS SDK ou AWS CLI oferece suporte para modificar as opções de metadados da instância nas instâncias existentes. Você não pode usar o console Amazon EC2 para modificar as opções de metadados da instância.

Como exigir o uso de IMDSv2

É possível optar por exigir que o IMDSv2 seja usado ao solicitar metadados de instância. Use o comando [modify-instance-metadata-options](#) da CLI e defina o parâmetro `http-tokens` como `required`. Quando você especifica um valor para `http-tokens`, você também deve definir `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-tokens required \  
  --http-endpoint enabled
```

Como alterar o limite de salto de resposta PUT

Para instâncias existentes, é possível alterar as configurações do limite de saltos de resposta de `PUT`. Use o comando [modify-instance-metadata-options](#) da CLI e defina o parâmetro `http-put-response-hop-limit` como o número de saltos necessário. No exemplo a seguir, o limite de saltos está definido como 3. Observe que ao especificar um valor para `http-put-response-hop-limit`, também é necessário definir `http-endpoint` como `enabled`.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-put-response-hop-limit 3 \  
  --http-endpoint enabled
```

Como restaurar o uso de IMDSv1 em uma instância usando IMDSv2

Você pode usar o comando da CLI [modify-instance-metadata-options](#) com `http-tokens` definido como `optional` para restaurar o uso de IMDSv1 ao solicitar metadados de instância.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-tokens optional \  
  --http-endpoint enabled
```

Como desabilitar o acesso aos metadados da instância

É possível desativar o acesso aos metadados da instância desabilitando o HTTP endpoint do serviço de metadados de instância, independentemente de qual versão do serviço de metadados de instância você está usando. É possível reverte essa alteração a qualquer momento habilitando o HTTP endpoint. Use o comando [modify-instance-metadata-options](#) da CLI e defina o parâmetro `http-endpoint` como `disabled`.

```
aws ec2 modify-instance-metadata-options \  
  --instance-id i-1234567898abcdef0 \  
  --http-endpoint disabled
```

```
--instance-id i-1234567898abcdef0 \
--http-endpoint disabled
```

Como controlar o uso de modify-instance-metadata-options

Para controlar quais usuários do IAM podem modificar as opções de metadados em uma instância existente, especifique uma política que impeça que todos os usuários que não tenham uma função especificada usem a API [ModifyInstanceMetadataOptions](#). Para ver um exemplo de política do IAM, consulte [Trabalhar com metadados de instância](#) (p. 1182).

Recuperar metadados da instância

Como os metadados da instância estão disponíveis em sua instância em execução, você não precisa usar o console do Amazon EC2 nem a AWS CLI. Isso pode ser útil quando você for elaborar scripts a serem executados a partir de sua instância. Por exemplo, você pode acessar o endereço IP local de sua instância a partir dos metadados da instância para gerenciar uma conexão com uma aplicação externa.

Os metadados da instância são divididos em categorias. Para obter uma descrição de cada categoria de metadados de instância, consulte [Categorias de metadados da instância](#) (p. 640).

Para visualizar todas as categorias de metadados da instância dentro de uma instância em execução, use o seguinte URI de IPv4 ou IPv6:

```
http://169.254.169.254/latest/meta-data/
```

```
http://[fd00:ec2::254]/latest/meta-data/
```

Os endereços IP são um endereço local de link e são válidos apenas a partir da instância. Para obter mais informações, consulte [Endereço local de link](#) na Wikipedia.

Note

Os exemplos nesta seção usam o endereço IPv4 do serviço de metadados da instância: 169.254.169.254. Se você estiver recuperando metadados de instância para instâncias do EC2 sobre o endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: fd00:ec2::254. O endereço IPv6 do serviço de metadados da instância é compatível com comandos IMDSv2. O endereço IPv6 só é acessível no [Instâncias criadas no Sistema Nitro](#) (p. 154).

O formato do comando é diferente dependendo de se IMDSv1 ou IMDSv2 é usado. Por padrão, é possível usar os dois serviços de metadados de instância. Para exigir o uso do IMDSv2, consulte [Usar IMDSv2](#) (p. 623).

Você pode usar cmdlets do PowerShell para recuperar o URI. Por exemplo, se você estiver executando a versão 3.0 ou posterior do PowerShell, use o seguinte cmdlet.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" =
"21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
```

Se você não quiser usar o PowerShell, instale uma ferramenta de terceiros, como o GNU Wget ou o cURL.

Important

Se você instalar uma ferramenta de terceiros em uma instância Windows, leia a documentação que a acompanha, pois o método de chamar o HTTP e o formato de saída podem ser diferentes do que está documentado aqui.

Observe que você não será cobrado pelas solicitações HTTP usadas para recuperar os metadados da instância e os dados do usuário.

Considerations

Para evitar problemas com a recuperação de metadados de instância, considere o seguinte:

- Os AWS SDKs usam chamadas IMDSv2 por padrão. Se a chamada IMDSv2 não receber resposta, o SDK tenta novamente o atendimento e, se houver falha, usa IMDSv1. Isso pode resultar em um atraso. Em um ambiente de contêiner, se o limite de salto for 1, a resposta de IMDSv2 não retorna porque ir ao contêiner é considerado um salto de rede adicional. Para evitar o processo de recuar para IMDSv1 e o atraso resultante, em um ambiente de contêiner recomendamos que você defina o limite de salto como 2. Para obter mais informações, consulte [Configurar as opções de metadados da instância \(p. 627\)](#).
- Se você executar uma instância do Windows usando uma AMI personalizada do Windows, para garantir que o serviço de metadados da instância funcione na instância, a AMI deverá ser uma imagem padronizada criada usando o [Sysprep \(p. 42\)](#). Caso contrário, o serviço de metadados da instância não funcionará.
- Para IMDSv2, você deve usar `/latest/api/token` ao recuperar o token. Emitir solicitações PUT para qualquer caminho específico da versão, por exemplo `/2021-03-23/api/token`, fará com que o serviço de metadados retorne erros 403 Forbidden. Este é o comportamento pretendido.

Respostas e mensagens de erro

Todos os metadados de instância são retornados como texto (tipo de conteúdo HTTP `text/plain`).

Uma solicitação para um recurso de metadados específico retorna o valor apropriado, ou um código de erro de HTTP 404 – `Not Found` se o recurso não estiver disponível.

Uma solicitação de um recurso de metadados geral (o URI termina com `/`) retorna uma lista de recursos disponíveis, ou um código de erro de HTTP 404 – `Not Found` se não houver esse recurso. Os itens da lista estão em linhas separadas que são delimitadas por caracteres de alimentação de linha (ASCII 10).

Para solicitações feitas usando o Serviço de metadados da instância versão 2, os seguintes códigos de erro HTTP podem ser retornados:

- 400 – `Missing or Invalid Parameters` – a solicitação PUT não é válida.
- 401 – `Unauthorized` – a solicitação GET usa um token inválido. A ação recomendada é gerar um novo token.
- 403 – `Forbidden` – a solicitação não é permitida ou o serviço de metadados da instância está desativado.

Exemplos de recuperação de metadados da instância

Exemplos

- [Obter as versões disponíveis dos metadados da instância \(p. 632\)](#)
- [Obter itens de metadados de nível superior. \(p. 633\)](#)
- [Obter a lista de chaves públicas disponíveis \(p. 635\)](#)

- Mostrar os formatos nos quais a chave pública 0 está disponível (p. 635)
- Obter a chave pública 0 (no formato de chave OpenSSH) (p. 635)
- Obter o ID de sub-rede de uma instância (p. 636)

Obter as versões disponíveis dos metadados da instância

Este exemplo obtém as versões disponíveis dos metadados da instância. Essas versões não se correlacionam necessariamente com uma versão de API do Amazon EC2. As versões anteriores estarão disponíveis caso você tenha scripts que contam com a estrutura e as informações presentes em uma versão anterior.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET - Uri http://169.254.169.254/  
1.0  
2007-01-19  
2007-03-01  
2007-08-29  
2007-10-10  
2007-12-15  
2008-02-01  
2008-09-01  
2009-04-04  
2011-01-01  
2011-05-01  
2012-01-12  
2014-02-25  
2014-11-05  
2015-10-20  
2016-04-19  
2016-06-30  
2016-09-02  
latest
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/  
1.0  
2007-01-19  
2007-03-01  
2007-08-29  
2007-10-10  
2007-12-15  
2008-02-01  
2008-09-01  
2009-04-04  
2011-01-01  
2011-05-01  
2012-01-12  
2014-02-25  
2014-11-05  
2015-10-20  
2016-04-19  
2016-06-30  
2016-09-02  
latest
```

Obter itens de metadados de nível superior.

Este exemplo obtém itens de metadados de nível superior. Para obter mais informações, consulte [Categorias de metadados da instância \(p. 640\)](#).

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET - Uri http://169.254.169.254/latest/meta-data/  
ami-id  
ami-launch-index  
ami-manifest-path  
block-device-mapping/  
hostname  
iam/  
instance-action  
instance-id  
instance-life-cycle  
instance-type  
local-hostname  
local-ipv4  
mac  
metrics/  
network/  
placement/  
profile  
public-hostname  
public-ipv4  
public-keys/  
reservation-id  
security-groups  
services/
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/  
ami-id  
ami-launch-index  
ami-manifest-path  
block-device-mapping/  
hostname  
iam/  
instance-action  
instance-id  
instance-type  
local-hostname  
local-ipv4  
mac  
metrics/  
network/  
placement/  
profile  
public-hostname  
public-ipv4  
public-keys/  
reservation-id  
security-groups  
services/
```

Os exemplos a seguir obtêm os valores de alguns dos itens de metadados de nível superior que foram obtidos no exemplo anterior. As solicitações do IMDSv2 usam o token armazenado que foi criado no comando do exemplo anterior, supondo-se que ele não expirou.

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -  
Uri http://169.254.169.254/latest/meta-data/ami-id  
ami-0abcdef1234567890
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id  
ami-0abcdef1234567890
```

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @ {"X-aws-ec2-metadata-token" = $token} -Method GET -  
Uri http://169.254.169.254/latest/meta-data/reservation-id  
r-0efghijk987654321
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-id  
r-0efghijk987654321
```

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @ {"X-aws-ec2-metadata-token" = $token} -Method GET -  
Uri http://169.254.169.254/latest/meta-data/local-hostname  
ip-10-251-50-12.ec2.internal
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-hostname  
ip-10-251-50-12.ec2.internal
```

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @ {"X-aws-ec2-metadata-token" = $token} -Method GET -  
Uri http://169.254.169.254/latest/meta-data/public-hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

Obter a lista de chaves públicas disponíveis

Este exemplo obtém uma lista de chaves públicas disponíveis.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET - Uri http://169.254.169.254/latest/meta-data/public-keys/0=my-public-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/0=my-public-key
```

Mostrar os formatos nos quais a chave pública 0 está disponível

Este exemplo mostra os formatos nos quais a chave pública 0 está disponível.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET - Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key openssh-key
```

Obter a chave pública 0 (no formato de chave OpenSSH)

Este exemplo obtém a chave pública 0 (no formato de chave OpenSSH).

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @ {"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @ {"X-aws-ec2-metadata-token" = $token} -Method GET - Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key ssh-rsa MIICiTCACfICQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMR AwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC01BTSDb25zb2x1MRIwEAYDVQ QDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEg5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMR AwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQ QKEwZBbWF6b24xFDASBgNVBAsTC01BTSDb25zb2x1MRIwEAYDVQ QDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEg5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIJ
```

```
21uUSfwfEvySwtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzzswY6786m86gpE
Ibb3OhjZnzcvQAArHndlQWIMm2nrAgMBAEwDQYJKoZlhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJ1J00zbhNYS5f6GuoEDmFJ10ZxBHjJnyp3780D8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
ssh-rsa MIICiTCACfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAOUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBASTC01BTSBdb25zb2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMxHzAd
BgkqhkiG9w0BCQEWEg5vb25lQGFtYXpbv15jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBASTC01BTSBDb25z
b2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEg5vb25lQGFt
YXpbv15jb20wg2QYJKoZlhvcNAQEFBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySwtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzzswY6786m86gpE
Ibb3OhjZnzcvQAArHndlQWIMm2nrAgMBAEwDQYJKoZlhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJ1J00zbhNYS5f6GuoEDmFJ10ZxBHjJnyp3780D8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Obter o ID de sub-rede de uma instância

Este exemplo obtém o ID de sub-rede para uma instância.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" =
"21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token

PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/network/interfaces/macs/02:29:96:8f:6a:2d/
subnet-id
subnet-be9b61d7
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/
interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Limitação de consulta

Limitamos consultas ao serviço de metadados da instância em uma base por instância, e limitamos o número de conexões simultâneas de uma instância com o serviço de metadados da instância.

Se você estiver usando o serviço de metadados de instância para recuperar as credenciais de segurança da AWS, evite consultar as credenciais durante cada transação ou simultaneamente em um número elevado de threads ou processos, pois isso pode levar a uma limitação. Em vez disso, recomendamos que você armazene em cache as credenciais até elas começarem a se aproximar da data de expiração.

Se você ficar limitado ao acessar o serviço de metadados de instância, tente a consulta novamente com uma estratégia de recuo exponencial.

Limitar o acesso a serviço de metadados da instância

É possível considerar o uso de regras do firewall local para desabilitar o acesso de alguns ou de todos os processos para o serviço de metadados de instância.

Note

Para [Instâncias criadas no Sistema Nitro \(p. 154\)](#), o IMDS pode ser acessível a partir de sua própria rede quando um dispositivo de rede em sua VPC, como um roteador virtual, encaminha pacotes para o endereço IMDS e a [verificação de origem/destino](#) padrão na instância está desativada. Para evitar que uma fonte de fora da VPC alcance o IMDS, recomendamos que você modifique a configuração do dispositivo de rede para descartar pacotes com o endereço IPv4 de destino do IMDS 169.254.169.254 e, se você ativou o endpoint IPv6, o endereço IPv6 do IMDS fd00:ec2::254.

Usar o firewall do Windows para limitar o acesso

O seguinte PowerShell de exemplo usa o firewall interno do Windows para impedir que o servidor Web do Servidor de informações da Internet (com base no ID de usuário de sua instalação padrão de NT AUTHORITY\IUSR) acesse 169.254.169.254. Ele usa uma regra de negação para rejeitar todas as solicitações de metadados de instância (IMDSv1 ou IMDSv2) de qualquer processo que execute como esse usuário.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT AUTHORITY\IUSR")
PS C:\> $BlockPrincipalsSID =
$blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalsDDL = "D:(A;;CC;;;$BlockPrincipalsSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalsDDL
```

Ou você pode considerar permitir o acesso apenas a usuários ou grupos específicos usando regras de permissão. As regras de permissão podem ser mais fáceis de gerenciar de uma perspectiva de segurança, porque elas exigem que você decida qual software precisa acessar os metadados de instância. Se você usar regras de permissão, haverá menos probabilidade de você permitir acidentalmente que o software acesse o serviço de metadados (que você não queria que tivesse acesso) se você alterar o software ou a configuração posteriormente em uma instância. Também é possível combinar o uso de grupos com regras de permissão, para que você possa adicionar ou remover usuários de um grupo com permissão sem precisar alterar a regra do firewall.

O exemplo a seguir impede o acesso aos metadados da instância por todos os processos em execução como um grupo do SO especificado na variável `blockPrincipal` (neste exemplo, o grupo Everyone do Windows), exceto os processos especificados em `exceptionPrincipal` (neste exemplo, um grupo chamado `trustworthy-users`). Você deve especificar as entidades de negação e de permissão porque o Firewall do Windows, ao contrário da regra `! --uid-owner trustworthy-user` nas iptables do Linux, não fornece um mecanismo de atalho para permitir somente uma entidade específica (usuário ou grupo) negando todas as outras.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
("Everyone")
PS C:\> $BlockPrincipalsSID =
$blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
$exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalsSID)"
```

```
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
#$blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalsDDL
```

Note

Para usar regras de firewall local, você precisa adaptar os comandos do exemplo anterior para se ajustarem a suas necessidades.

Usar regras de netsh para limitar o acesso

É possível considerar o bloqueio de todos os softwares usando regras de netsh, mas essas regras são muito menos flexíveis.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether" dir=out
protocol=TCP remoteip=169.254.169.254 action=block
```

Note

- Para usar regras de firewall local, você precisa adaptar os comandos do exemplo anterior para se ajustarem a suas necessidades.
- netshAs regras de devem ser definidas em um prompt de comando elevado e não podem ser definidas para negar ou permitir principais específicos.

Trabalhar com dados do usuário da instância

Ao trabalhar com dados do usuário da instância, lembre-se do seguinte:

- Os dados do usuário devem ser codificados por base64. O console do Amazon EC2 pode executar a codificação base64 para você ou aceitar a entrada codificada por base64.
- Os dados do usuário são limitados a 16 KB, na forma bruta, antes de serem codificados em base64. O tamanho de uma string de comprimento n depois que a codificação em base64 for ceil (n/3)*4.
- Os dados do usuário devem ser decodificados em base64 quando você os recupera. Se você recuperar os dados usando o console ou os metadados da instância, eles serão decodificados automaticamente para você.
- Os dados do usuário são tratados como dados opacos: o que você fornece é o que receberá de volta. Cabe à instância interpretá-los.
- Se você interromper uma instância, modificar os dados do usuário e iniciar a instância, os dados do usuário atualizados não serão executados automaticamente quando você iniciar a instância. No entanto, você pode definir as configurações para que os scripts de dados do usuário atualizados sejam executados uma vez ao iniciar a instância ou sempre que reiniciar ou iniciar a instância.

Especificar os dados do usuário da instância na inicialização

Você pode especificar dados do usuário quando você executar uma instância. Você pode especificar que os dados do usuário serão executados uma vez na execução ou sempre que você reiniciar ou iniciar a instância. Para obter mais informações, consulte [Executar comandos na instância do Windows na inicialização \(p. 614\)](#).

Modificar os dados do usuário da instância

Você poderá modificar os dados do usuário de uma instância em estado interrompido se o volume raiz for um volume do EBS. Para obter mais informações, consulte [Visualizar e atualizar os dados do usuário da instância \(p. 619\)](#).

Recuperar os dados do usuário da instância

Note

Os exemplos nesta seção usam o endereço IPv4 do serviço de metadados da instância: 169.254.169.254. Se você estiver recuperando metadados de instância para instâncias do EC2 sobre o endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: fd00:ec2::254. O endereço IPv6 do serviço de metadados da instância é compatível com comandos IMDSv2. O endereço IPv6 só é acessível no [Instâncias criadas no Sistema Nitro \(p. 154\)](#).

Para recuperar os dados do usuário de uma instância em execução, use o seguinte URI.

```
http://169.254.169.254/latest/user-data
```

Uma solicitação de dados do usuário retorna os dados no estado em que se encontram (tipo de conteúdo application/octet-stream).

Este exemplo retorna os dados do usuário que foram fornecidos como texto separado por vírgulas.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET - Uri http://169.254.169.254/latest/user-data  
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod - Headers @ {"X-aws-ec2-metadata-token-ttl-seconds" = "21600"}  
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri  
http://169.254.169.254/latest/user-data  
1234,john,reboot,true | 4512,richard, | 173,,,
```

Este exemplo retorna os dados de usuário que foram fornecidos como um script.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @ {"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @ {"X-aws-ec2-metadata-token" = $token} -Method GET - Uri http://169.254.169.254/latest/user-data  
<powershell>  
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")  
New-Item $file -ItemType file  
</powershell>  
<persist>true</persist>
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/user-data  
<powershell>  
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")  
New-Item $file -ItemType file
```

```
</powershell>
<persist>true</persist>
```

Para recuperar dados do usuário em uma instância no seu computador, consulte [Dados do usuário e Tools for Windows PowerShell \(p. 620\)](#).

Recuperar dados dinâmicos

Para recuperar dados dinâmicos de uma instância em execução, use o seguinte URL.

```
http://169.254.169.254/latest/dynamic/
```

Note

Os exemplos nesta seção usam o endereço IPv4 do serviço de metadados da instância: 169.254.169.254. Se você estiver recuperando metadados de instância para instâncias do EC2 sobre o endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: fd00:ec2::254. O endereço IPv6 do serviço de metadados da instância é compatível com comandos IMDSv2. O endereço IPv6 só é acessível no [Instâncias criadas no Sistema Nitro \(p. 154\)](#).

Este exemplo mostra como recuperar as categorias de identidade de instância de alto nível.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" =
"21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token

PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
pkcs7
signature
```

Para obter mais informações sobre dados dinâmicos e os exemplos de como recuperá-los, consulte [Documentos de identidade da instância \(p. 648\)](#).

Categorias de metadados da instância

Os metadados da instância são divididos em categorias. Quando você recupera metadados de instância, estes são os itens de nível superior.

Quando o Amazon EC2 libera uma nova categoria de metadados de instância, os metadados de instância da nova categoria podem não estar disponíveis para instâncias existentes. Com instâncias criadas no [Sistema Nitro \(p. 154\)](#), é possível recuperar metadados de instância somente para as categorias que estavam disponíveis ao iniciar. Para instâncias com o hipervisor Xen, é possível [interromper e iniciar \(p. 455\)](#) a instância para atualizar as categorias que estão disponíveis para a instância.

A tabela a seguir lista as categorias de metadados da instância. Alguns dos nomes de categoria incluem espaços reservados para dados exclusivos da instância. Por exemplo, *mac* representa o endereço MAC para a interface de rede. É necessário substituir os espaços reservados pelos valores reais ao recuperar os metadados da instância.

Dados	Descrição	Versão
<code>ami-id</code>	O ID da AMI usada para executar a instância.	1,0
<code>ami-launch-index</code>	Se você iniciou mais de uma instância ao mesmo tempo, esse valor indicará a ordem na qual a instância foi executada. O valor da primeira instância executada é 0.	1,0
<code>ami-manifest-path</code>	O caminho para o arquivo de manifesto da AMI no Amazon S3. Se você usou uma AMI baseada no Amazon EBS para executar a instância, o resultado retornado será <code>unknown</code> .	1,0
<code>ancestor-ami-ids</code>	Os IDs das AMIs de todas as instâncias que foram reagrupadas para criar essa AMI. Este valor existirá somente se o arquivo de manifesto de AMIs continham uma chave <code>ancestor-ami</code> .	10/10/2007
<code>block-device-mapping/ami</code>	O dispositivo virtual que contém o sistema de arquivos de inicialização/raiz.	15/12/2007
<code>block-device-mapping/ebs N</code>	Os dispositivos virtuais associados a quaisquer volumes do Amazon EBS. Os volumes do Amazon EBS estarão disponíveis somente em metadados se estiverem presentes no momento da execução ou quando a instância foi iniciada pela última vez. O N indica o índice do volume do Amazon EBS (como <code>ebs1</code> ou <code>ebs2</code>).	15/12/2007
<code>block-device-mapping/eph emeral N</code>	Os dispositivos virtuais para qualquer volume de armazenamento de instâncias não NVMe. O N indica o índice de cada volume. O número dos volumes de armazenamento de instâncias no mapeamento de dispositivos de blocos pode não corresponder ao número real de volumes de armazenamento de instâncias da instância. O tipo de instância determina o número de volumes de armazenamento de instâncias que estão disponíveis para uma	15/12/2007

Dados	Descrição	Versão
	instância. Se o número de volumes de armazenamento de instâncias em um mapeamento de dispositivos de blocos exceder o número disponível para uma instância, os volumes de armazenamento de instâncias adicionais serão ignorados.	
block-device-mapping/root	Os dispositivos virtuais ou as partições associadas aos dispositivos raiz, ou as partições no dispositivo virtual, onde o sistema de arquivos raiz (/ ou C:) está associado à instância específica.	15/12/2007
block-device-mapping/swap	Os dispositivos virtuais associados a swap. Nem sempre presente.	15/12/2007
elastic-gpus/ associations/ <i>elastic-gpu-id</i>	Se houver um Elastic GPU anexado à instância, ele contém uma string JSON com informações sobre o Elastic GPU, incluindo suas informações de ID e conexão.	30/11/2016
elastic-inference/ associations/ <i>eia-id</i>	Se houver um acelerador do Elastic Inference anexado à instância, ele conterá uma string JSON com informações sobre o acelerador do Elastic Inference, incluindo o ID e o tipo.	29/11/2018
events/maintenance/history	Se houver eventos de manutenção da instância concluídos ou cancelados, contém uma string JSON com informações sobre os eventos. Para obter mais informações, consulte Para visualizar o histórico de eventos sobre eventos concluídos ou cancelados (p. 878) .	17/08/2018
events/maintenance/scheduled	Se houver eventos de manutenção da instância ativos, contém uma string JSON com informações sobre os eventos. Para obter mais informações, consulte Visualizar eventos agendados (p. 875) .	17/08/2018

Dados	Descrição	Versão
<code>events/recommendations/rebalance</code>	O tempo aproximado, em UTC, quando a notificação de recomendação de rebalanceamento da instância do EC2 é emitida para a instância. Veja a seguir um exemplo dos metadados para esta categoria: { "noticeTime": "2020-11-05T08:22:00Z" }. Esta categoria só está disponível após a emissão da notificação. Para obter mais informações, consulte Recomendações de rebalanceamento de instâncias do EC2 (p. 333) .	04-11-2020
<code>hostname</code>	O nome de host DNS IPv4 privado da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0).	Versão 1.0
<code>iam/info</code>	Se houver uma função do IAM associada à instância, conterá informações sobre a última vez que o perfil de instância foi atualizado, incluindo a data <code>LastUpdated</code> , <code>InstanceProfileArn</code> e <code>InstanceProfileId</code> . Caso contrário, não estará presente.	12/01/2012
<code>iam/security-credentials/role-name</code>	Se houver uma função do IAM associada à instância, <code>role-name</code> será o nome da função, e <code>role-name</code> conterá as credenciais de segurança temporárias associadas à função (para obter mais informações, consulte Recuperar credenciais de segurança dos metadados da instância (p. 1196)). Caso contrário, não estará presente.	12/01/2012
<code>identity-credentials/ec2/info</code>	[Somente uso interno] Informações sobre as credenciais em <code>identity-credentials/ec2/security-credentials/ec2-instance</code> . Essas credenciais são usadas por recursos da AWS, como EC2 Instance Connect, e não têm permissões adicionais de API da AWS nem privilégios além da identificação da instância.	23/05/2018

Dados	Descrição	Versão
<code>identity-credentials/ec2/security-credentials/ec2-instance</code>	[Somente uso interno] Credenciais que permitem que o software na instância se identifique na AWS para oferecer suporte a recursos como EC2 Instance Connect. Essas credenciais não têm permissões nem privilégios adicionais de API da AWS.	23/05/2018
<code>instance-action</code>	Notifica a instância que ela deve ser reinicializada em preparação para o empacotamento. Valores válidos: <code>none</code> <code>shutdown</code> <code>bundle-pending</code> .	01/09/2008
<code>instance-id</code>	O ID dessa instância.	Versão 1.0
<code>instance-life-cycle</code>	A opção de compra desta instância. Para obter mais informações, consulte Opções de compra de instância (p. 253) .	01/10/2019
<code>instance-type</code>	O tipo da instância. Para obter mais informações, consulte Tipos de instância (p. 149) .	29/08/2007
<code>kernel-id</code>	O ID do kernel executado com essa instância, se aplicável.	01/02/2008
<code>local-hostname</code>	O nome de host DNS IPv4 privado da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0).	19/01/2007
<code>local-ipv4</code>	O endereço IPv4 privado da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0).	Versão 1.0
<code>mac</code>	O endereço Media Access Control (MAC) da instância. Em casos em que várias interfaces de rede estão presentes, isso se refere ao dispositivo eth0 (o dispositivo para o qual o número de dispositivo é 0).	01/01/2011
<code>metrics/vhostmd</code>	Não está mais disponível.	01/05/2011

Dados	Descrição	Versão
<code>network/interfaces/macs/mac/device-number</code>	O número de dispositivo exclusivo associado a essa interface. O número do dispositivo corresponde ao nome do dispositivo; por exemplo, um <code>device-number</code> de 2 é para o dispositivo <code>eth2</code> . Essa categoria corresponde aos campos <code>DeviceIndex</code> e <code>device-index</code> que são usados pelos comandos da API do Amazon EC2 e do EC2 para a AWS CLI.	01/01/2011
<code>network/interfaces/macs/mac/interface-id</code>	O ID da interface de rede.	01/01/2011
<code>network/interfaces/macs/mac/ipv4-associations/public-ip</code>	Os endereços IPv4 privados que estão associados a cada endereço IP público e estão atribuídos a essa interface.	01/01/2011
<code>network/interfaces/macs/mac/ipv6s</code>	Os endereços IPv6 associados à interface. Retornados apenas para instâncias executadas em uma VPC.	30/06/2016
<code>network/interfaces/macs/mac/local-hostname</code>	O nome do host local da interface.	01/01/2011
<code>network/interfaces/macs/mac/local-ipv4s</code>	Os endereços IPv4 privados associados à interface.	01/01/2011
<code>network/interfaces/macs/mac/mac</code>	O endereço MAC da instância.	01/01/2011
<code>network/interfaces/macs/mac/network-card-index</code>	O índice da placa de rede. Alguns tipos de instância suportam várias placas de rede.	01-11-2020
<code>network/interfaces/macs/mac/owner-id</code>	O ID do proprietário da interface de rede. Em ambientes de várias interfaces, um terceiro pode anexar uma interface, como o Elastic Load Balancing. O tráfego em uma interface é sempre cobrado do proprietário da interface.	01/01/2011
<code>network/interfaces/macs/mac/public-hostname</code>	O DNS público da interface (IPv4). Essa categoria só será retornada se o atributo <code>enableDnsHostnames</code> for definido como <code>true</code> . Para obter mais informações, consulte Using DNS with Your VPC .	01/01/2011
<code>network/interfaces/macs/mac/public-ipv4s</code>	Os endereços IP públicos ou os endereços IP elásticos associados à interface. Pode haver vários endereços IPv4 em uma instância.	01/01/2011

Dados	Descrição	Versão
<code>network/interfaces/macs/mac/security-groups</code>	Security groups aos quais a interface de rede pertence.	01/01/2011
<code>network/interfaces/macs/mac/security-group-ids</code>	Os IDs dos security groups aos quais a interface de rede pertence.	01/01/2011
<code>network/interfaces/macs/mac/subnet-id</code>	O ID da sub-rede na qual a interface reside.	01/01/2011
<code>network/interfaces/macs/mac/subnet-ipv4-cidr-block</code>	O bloco CIDR IPv4 da sub-rede na qual a interface reside.	01/01/2011
<code>network/interfaces/macs/mac/subnet-ipv6-cidr-blocks</code>	O bloco CIDR IPv6 da sub-rede na qual a interface reside.	30/06/2016
<code>network/interfaces/macs/mac/vpc-id</code>	O ID da VPC na qual a interface reside.	01/01/2011
<code>network/interfaces/macs/mac/vpc-ipv4-cidr-block</code>	O bloco CIDR IPv4 principal da VPC.	01/01/2011
<code>network/interfaces/macs/mac/vpc-ipv4-cidr-blocks</code>	Os blocos CIDR IPv4 da VPC.	30/06/2016
<code>network/interfaces/macs/mac/vpc-ipv6-cidr-blocks</code>	O bloco CIDR IPv6 da VPC na qual a interface reside.	30/06/2016
<code>placement/availability-zone</code>	A zona de disponibilidade na qual a instância foi executada.	01/02/2008
<code>placement/availability-zone-id</code>	O ID estático da zona de disponibilidade em que a instância é executada. O ID da zona de disponibilidade é consistente entre as contas. No entanto, pode ser diferente da zona de disponibilidade, que pode variar de acordo com a conta.	24/08/2020
<code>placement/group-name</code>	O nome do grupo de posicionamento no qual a instância é executada.	24/08/2020
<code>placement/host-id</code>	O ID do host no qual a instância é executada. Aplicável apenas a Hosts dedicados.	24/08/2020
<code>placement/partition-number</code>	O número da partição na qual a instância é executada.	24/08/2020
<code>placement/region</code>	A região da AWS na qual a instância é executada.	24/08/2020
<code>product-codes</code>	AWS Marketplace Os códigos de produtos associados com a instância, se houver.	01/03/2007

Dados	Descrição	Versão
public-hostname	O DNS público da instância. Essa categoria só será retornada se o atributo <code>enableDnsHostnames</code> for definido como <code>true</code> . Para obter mais informações, consulte Usar DNS com a VPC , no Guia do usuário da Amazon VPC.	19/01/2007
public-ipv4	O endereço IPv4 público. Se um endereço IP elástico estiver associado à instância, o valor retornado será o endereço IP elástico.	19/01/2007
public-keys/0/openssh-key	Chave pública. Disponível somente se fornecido no momento da execução da instância.	Versão 1.0
ramdisk-id	O ID do disco de RAM no momento da execução, se aplicável.	10/10/2007
reservation-id	O ID da reserva.	Versão 1.0
security-groups	Os nomes dos security groups aplicados à instância. Após a execução, você só pode alterar os grupos de segurança das instâncias. Essas alterações estão refletidas aqui e em <code>network/interfaces/mac/<i>mac</i>/security-groups</code> .	Versão 1.0
services/domain	O domínio dos recursos da AWS para a região.	25/02/2014
services/partition	A partição na qual o recurso está. Para Regiões padrão da AWS a partição é <code>aws</code> . Se você tem recursos em outras partições, a partição é <code>aws-<i>partitionname</i></code> . Por exemplo, a partição de recursos na região China (Pequim) é <code>aws-cn</code> .	20/10/2015
spot/instance-action	A ação (hibernar, interromper ou encerrar) e o tempo aproximado, em UTC, em que a ação ocorrerá. Esse item estará presente somente se a instância spot tiver sido marcada para hibernar, interromper ou encerrar. Para obter mais informações, consulte instance-action (p. 342) .	15/11/2016

Dados	Descrição	Versão
spot/termination-time	O tempo aproximado, em UTC, no qual o sistema operacional para sua instância spot receberá o sinal de desligamento. Esse item está presente e contém um valor de tempo (por exemplo, 2015-01-05T18:02:00Z) somente se a instância spot tiver sido marcada para término pelo Amazon EC2. O item hora de encerramento não está definido como uma hora se você mesmo encerrou a instância spot. Para obter mais informações, consulte termination-time (p. 342) .	05/11/2014

Categorias de dados dinâmicos

A tabela a seguir lista as categorias de dados dinâmicos.

Dados	Descrição	Versão
fws/instance-monitoring	O valor que mostra se o cliente habilitou o monitoramento de um minuto detalhado no CloudWatch. Valores válidos: enabled disabled	04/04/2009
instance-identity/document	O JSON que contém os atributos da instância, como o ID da instância, o endereço IP privado, etc. Consulte Documentos de identidade da instância (p. 648) .	04/04/2009
instance-identity/pkcs7	Usado para verificar a autenticidade e o conteúdo do documentos em relação à assinatura. Consulte Documentos de identidade da instância (p. 648) .	04/04/2009
instance-identity/signature	Os dados que podem ser usados por outras partes para verificar sua origem e autenticidade. Consulte Documentos de identidade da instância (p. 648) .	04/04/2009

Documentos de identidade da instância

Cada instância iniciada tem um documento de identidade da instância que fornece informações sobre a própria instância. É possível usar o documento de identidade da instância para validar os atributos da instância.

O documento de identidade da instância é gerado quando a instância é interrompida e iniciada, reiniciada ou lançada. O documento de identidade da instância é exposto (no formato JSON de texto simples) por meio do serviço de metadados de instância. O endereço IPv4 do 169.254.169.254 é um endereço local de link e é válido apenas a partir da instância. Para obter mais informações, consulte [Endereço local de link](#) na Wikipedia. O endereço IPv6 do fd00:ec2::254 é um endereço local único e é válido apenas a partir da instância. Para obter mais informações, consulte [Endereço local único](#) na Wikipédia.

Note

Os exemplos nesta seção usam o endereço IPv4 do serviço de metadados da instância: 169.254.169.254. Se você estiver recuperando metadados de instância para instâncias do

EC2 sobre o endereço IPv6, certifique-se de habilitar e usar o endereço IPv6: `fd00:ec2::254`. O endereço IPv6 do serviço de metadados da instância é compatível com comandos IMDSv2. O endereço IPv6 só é acessível no [Instâncias criadas no Sistema Nitro \(p. 154\)](#).

É possível recuperar o documento de identidade da instância de uma instância em execução a qualquer momento. O documento de identidade da instância inclui as seguintes informações:

Dados	Descrição
<code>devpayProductCodes</code>	Suspenso.
<code>marketplaceProductCodes</code>	O código do produto AWS Marketplace da AMI usada para iniciar a instância.
<code>availabilityZone</code>	A zona de disponibilidade na qual a instância está em execução.
<code>privateIp</code>	O endereço IPv4 privado da instância.
<code>version</code>	A versão do formato do documento de identidade da instância.
<code>instanceId</code>	O ID da instância.
<code>billingProducts</code>	Os produtos de faturamento da instância.
<code>instanceType</code>	O tipo de instância da instância.
<code>accountId</code>	O ID da conta da AWS que iniciou a instância.
<code>imageId</code>	A ID do AMI usado para executar a instância.
<code>pendingTime</code>	A data e a hora em que a instância foi iniciada.
<code>architecture</code>	A arquitetura da AMI usada para iniciar a instância (i386 x86_64 arm64).
<code>kernelId</code>	O ID do kernel associado à instância, se aplicável.
<code>ramdiskId</code>	O ID do disco de RAM associado a essa instância, se aplicável.
<code>region</code>	A região em que a instância está em execução.

Recuperar o documento de identidade da instância de texto sem formatação

Como recuperar o documento de identidade da instância de texto simples

Conecte-se à instância e execute um dos comandos a seguir, dependendo da versão do serviço de metadados de instância (IMDS) usada pela instância.

IMDSv2

```
PS C:\> $Token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/token).Content
```

```
PS C:\> (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

IMDSv1

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

A seguir está um exemplo de saída.

```
{  
    "devpayProductCodes" : null,  
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],  
    "availabilityZone" : "us-west-2b",  
    "privateIp" : "10.158.112.84",  
    "version" : "2017-09-30",  
    "instanceId" : "i-1234567890abcdef0",  
    "billingProducts" : null,  
    "instanceType" : "t2.micro",  
    "accountId" : "123456789012",  
    "imageId" : "ami-5fb8c835",  
    "pendingTime" : "2016-11-19T16:32:11Z",  
    "architecture" : "x86_64",  
    "kernelId" : null,  
    "ramdiskId" : null,  
    "region" : "us-west-2"  
}
```

Verifique o documento de identidade da instância

Se você pretende usar o conteúdo do documento de identidade da instância para um propósito importante, deve verificar seu conteúdo e autenticidade antes de usá-lo.

O documento de identidade da instância de texto simples é acompanhado por três assinaturas hash e criptografadas. É possível usar essas assinaturas para verificar a origem e a autenticidade do documento de identidade da instância e as informações incluídas nele. São fornecidas as seguintes assinaturas:

- Assinatura codificada em base64 – trata-se de um hash SHA256 codificado em base64 do documento de identidade da instância que é criptografado usando um par de chaves RSA.
- Assinatura PKCS7 – trata-se de um hash SHA1 do documento de identidade da instância que é criptografado usando um par de chaves DSA.
- Assinatura RSA-2048 – trata-se de um hash SHA256 do documento de identidade da instância que é criptografado usando um par de chaves RSA-2048.

Cada assinatura está disponível em um endpoint diferente nos metadados da instância. É possível usar qualquer uma dessas assinaturas dependendo dos requisitos de hash e criptografia. Para verificar as assinaturas, é necessário usar o certificado público da AWS correspondente.

Important

Para validar o documento de identidade da instância usando a assinatura codificada em base64 ou assinatura RSA2048, você deve solicitar o certificado público da AWS correspondente do [AWS Support](#).

Os tópicos a seguir fornecem etapas detalhadas para validar o documento de identidade da instância usando cada assinatura.

- [Usar a assinatura PKCS7 para verificar o documento de identidade da instância \(p. 650\)](#)
- [Usar a assinatura codificada em base64 para verificar o documento de identidade da instância \(p. 655\)](#)
- [Usar a assinatura RSA-2048 para verificar o documento de identidade da instância \(p. 658\)](#)

Usar a assinatura PKCS7 para verificar o documento de identidade da instância

Este tópico explica como verificar o documento de identidade da instância usando a assinatura PKCS7 e o certificado público DSA da AWS.

Prerequisites

Este procedimento exige a classe `System.Security` Microsoft .NET Core. Para adicionar a classe à sessão do PowerShell, execute o comando a seguir.

```
PS C:\> Add-Type -AssemblyName System.Security
```

Note

O comando adiciona a classe somente à sessão atual do PowerShell. Se você iniciar uma nova sessão, deverá executar o comando novamente.

Como verificar o documento de identidade da instância usando a assinatura PKCS7 e o certificado público DSA da AWS

1. Conecte-se à instância.
2. Recupere a assinatura PKCS7 dos metadados da instância, converta-a em uma matriz de bytes e adicione-a a uma variável chamada `$Signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
PS C:\> $Token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância, converta-o em uma matriz de bytes e adicione-o a uma variável chamada `$Document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Crie um arquivo chamado `certificate.pem` e adicione um dos certificados públicos DSA da AWS a seguir, dependendo da região.

Other AWS Regions

O certificado público da AWS a seguir se destina a todas as regiões da AWS, exceto Hong Kong, Bahrein, China e GovCloud.

```
-----BEGIN CERTIFICATE-----  
MIIC7TCCAq0CCQCWukjZ5V4aZZAJBgcqhkJOOAQDMFwxCzAJBgNVBAYTA1VTMRkw
```

```
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIEzMqzaeFw0xMjAxMDUxMjU2MTJaFw0z  
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u  
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNl  
cnZpY2VzIEzMqzCCAbcgwgEsBgcqhkjOOAQBMIIBhKBgQCjkvcS2bb1VQ4yt/5e  
ih5006kK/n1Lz1lr7D8ZwtQP8fOEpp5E2ng+D6UD1Z1gYipr58Kj3nssSNpI6bX3  
Vy1QzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P  
hviyt5JH/nY14h3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j  
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAoXau8Qe+MbcJ1/U  
hhy1KHvpCG19fueQ2s6IL0Ca0/buycu1CiYQk40KNHCChfNiZbdlx1E9rpUp7bnF  
1Ra2v1ntMX3caRVDdtPEWmdxSCYsYFDk4mzrOlBA4GEAAkBgEbmeve5f8LIE/Gf  
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BPPqeZqpWRa5P/+jrdKml1qx4llHW  
MXrs3IgIb6+hUIB+S8dz8/mm0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw  
vSeDCouMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAaLAIUWXBlk40xtTwSw  
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K  
-----END CERTIFICATE-----
```

Hong Kong Region

O certificado público da AWS da região Hong Kong é o seguinte:

```
-----BEGIN CERTIFICATE-----  
MIIC7zCCAq4CCQC07MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw  
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIEzMqzaeFw0xOTAYMDMwMjIxMjFaFw00  
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u  
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNl  
cnZpY2VzIEzMqzCCAbcgwgEsBgcqhkjOOAQBMIIBhKBgQDvQ9RzVvf4MAwGbqfx  
b1CvCoVb99570kLGn/04CowHXJ+vTBR7eyIa6AoXltsQXB0mrJswToFKKxT4gbuw  
jk7s9QX4CmTRwCEgO2RxtZSVjOhsUQMh+yf7ht4OVL97LWnNfGsX2cwyjcrWHYgI  
71vnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOOG  
eSNmpw4QFu4pI1Aykm6EnTZKKHT87gdXkAkfoC5fAfOxxhne2HezHpw9ap2tMV5  
8bWNvoPHvoKCQqfm+OUBLaxC/3vqoVkJL2mG1KgUH9+hrtpMTkwO3REnKe7I50  
x9qDimJpOihrl4I0dYvy9xUOoz+DzFAW8+y1WVYpA4GFAAKBqODbnBAKSxWr9QHY  
6Dt+EFdGz61AZLedeBKpaP53Z1DT034J0C55YbtwBTFGqPtOLxnUVd1GiD6GbmC  
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ  
9pdou/ibRPH11E2nz6pK7GbQ0tLyHTAJBgcqhkjOOAQDAzAACM0CFQCoJlwGtJQC  
cLoM4p/jtVF0j26xbgIUS4pDKyHaG/eaygLttFpFJqzWhc=  
-----END CERTIFICATE-----
```

Bahrain Region

O certificado público da AWS da região Bahrain é o seguinte:

```
-----BEGIN CERTIFICATE-----  
MIIC7jCCAq4CCQCWVigSmP8RhtAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw  
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIEzMqzaeFw0xOTAYMDUxMzA2MjFaFw00  
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u  
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNl  
cnZpY2VzIEzMqzCCAbcgwgEsBgcqhkjOOAQBMIIBhKBgQDcwojQfgWdV1Qlo0OB  
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q  
PH1P1WGL8IZ34BUGRTtG4tVolvp0smjkMvyRu5hIdKtzjv93Ccx15gVgyk+o1IEG  
fZ2Kbw/Dd8JfoPS7KaSCmJKxQIVAIzbIaDFRGA2qcMkW2HWASyND17bAoGBAnTz  
IdhMq+l2I5iofy2oj3HI21kj3LtzrWEg3W+/4rvhL31TmOnne1rl9yGujrjQwy5  
Zp9V4A/w9w2010Lx4K6hj34Efey/aQnZwNdNhv/FQP7Az0fju+Y16L1300HOrL0z  
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBqOCVS7m77nuNALZ8  
wvUqcooxXMPKxJF154NxAsAu19KP9KN4svm003Zrb7t2F0tXRM8zU3TqMpryq1o5  
mpMpsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr  
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGwm5ED1  
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==  
-----END CERTIFICATE-----
```

Cape Town Region

O certificado público da AWS da região Cidade do Cabo é o seguinte:

```
-----BEGIN CERTIFICATE-----  
MIIC7DCCAwCCQCnbcCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw  
FwYDVQQIExBXYXNaoW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFNlcnPZpY2VzIEzMqzaEfw0xOTA2MDQxMjQ4MDVaFw00  
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXNaoW5ndG9u  
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1  
cnZpY2VzIEzMqzaEfw0xOTA2MDQxMjQ4MDVaFw00NTA2MDQxMjQ4MDVaFw00  
pQSCMHwmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8jWG5uR4TXRzmZpGpmXB  
bSuFAR6BGqud2LnT/HIWGJAsnX2u0tSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw  
qO6TlnExHFVj8LMkylZgiaElCQIVAIhdobse4K0QnbAhCLER2euQzloXAoGAV/21  
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TengLQi5iccn/7EIfNtvVO5TZKuIKq7J  
gXzr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq  
ekfe15jinaX8MsKUdyDK7Y+iFCG4Pvh0M4+W2XwDgYQAAoGAIxOKbVgwLxrn6Pi2  
6hBoihFv16jKxQ10hHzXJL0Vvy9QwnqjJJRF0Cy3dB0zicLxiIxelIdYfvqJr+u  
h1N8rGxEZYyJBEUKMGvscODW85jonXz0bNfcP0aaKH01KKVJL+OZi5n2kn9wgdo5  
F3CVnM18BuRa8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADASAhQfa7MCJZ+/TEY5  
AUr0J4wm8VzjoAIUSYzVu2NdRJ/ERPmDfhW5Esjh1CA=-----END CERTIFICATE-----
```

Milan Region

O certificado público da AWS da região Milão é o seguinte:

```
-----BEGIN CERTIFICATE-----  
MIIC7TCCAqwcCQCME1HPdwG37jaJBgcqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw  
FwYDVQQIExBXYXNaoW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFNlcnPZpY2VzIEzMqzaEfw0xOTA0MjkyMDM1MjJaFw00  
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXNaoW5ndG9u  
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1  
cnZpY2VzIEzMqzaEfw0xOTA0MjkyMDM1MjJaFw00NTA0MjkyMDM1MjJaFw00  
NPfeEk94eiCQA5xNONu7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0  
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJmT  
HJSKSSvUgpdDIRvJXuyB0zdB+wIVALQ3OLeVGd1PMNfs1nD/Yyn+32wNaOGAPBQ3  
7XHg5NLOS4326eFRUT+4ornqFjjP6dp3pOBEPzIpNmZTtkCNNUKE4Go9hv5T4lh  
R0pODVwV0CUpMAZVBp9Obp1PCyEZtuDqVa7ukPOUpQNqOhLLAqkigTyXVOSmt  
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwjkPAdgYQAAoGAV10EQPYQUG5/M3xf  
6vE7jKTxxjFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2oZVUKzWo  
wDUbeu65DcRdwzrSwCbBTU34s1tFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBelv  
uaMQmgOYeZ5e0f104GtqPl+1hcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+  
AeBK+j6m2h9SKQIVAIbnHs2a8cQVABDCQXVXrc0tOm08-----END CERTIFICATE-----
```

China Regions

O certificado público da AWS para as regiões China (Pequim) e China (Ningxia) é o seguinte.

```
-----BEGIN CERTIFICATE-----  
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsfADBCMQswCQYDVQQGEwJV  
UzEZMBcGA1UECBMQV2FzaGluZ3RvbIBTDGF0ZTEQMA4GA1UEBxMHU2VhdHRSZTEg  
MB4GA1UEChMXQW1hem9uIFd1YiBTZXJ2aWN1cyBMTEMwIBcNMTUwNTEzMDk1OTE1  
WhgPMjE5NDEwMTYwOTU5MTVamFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXN0  
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24g  
V2ViIFNlcnPZpY2VzIEzMqzaCCASIwDQYJKoZIhvCNQEBBQADggEPADCCAQoCggEB  
AMWk9vypSmDU3AxZ2Cy2bvKeK3F1UqNpMuyerizi+NTs8tQqtNloaQcqhto/l  
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNLJ2fvImWyWe2f2Kq/BL917N7C  
P2ZT52/sH9orlck1n2z08xPi7MItgPHQwu30xsGQsAdWucdxjHGtdchulpo1uJ31  
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r-----END CERTIFICATE-----
```

```
vtBj/SM4/IgQ3xJslFc190TzbQbgxiI88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWf0dy0+OoECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdszN2+0E
V1BFr3DPWJHWrf1b7z1+1X/ZseW2hYE5r6xrLv+1VPf/L5I6kB7GETqhzUqteY7
zAeoLrVu/70ynRyfQetJVGichaaxLNm3lcr6kcxOowb+WQO84cwrB3keykH4gRX
KHB2rlWSxta+2panSE01JX2q5jhcfP90rDOTZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbOp1peGC19idOUqxPxWsasWxQX0azYsP
9RyWLHKxH1dMuA==

-----END CERTIFICATE-----
```

GovCloud Regions

O certificado público da AWS para as regiões GovCloud da AWS é o seguinte.

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzABgNVBAYTA1VTMRkw
FwyDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViFNlcnPzY2VzIEkMQzaeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzABgNVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViFN1
cnZpY2VzIEkMQzCCAbcwggEsBgcqhkjOOAQBMIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5006kK/n1Lz1lr7D8ZwtQP8fOEpp5E2ng+D6UD1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tKqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAoTXau8Qe+MBcJ1/U
hy1KHVpCG19fueQ2s6IL0Ca0/buycU1ClYQk40KNHCchfNiZbdIx1E9rpUp7bnF
1Ra2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTeb5+k2tn92BBPqeZqpWRa5P/+jrdKm1lqx411HW
MXrs3IgIb6+hUIB+S8dz8/mm0Obpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCouMYQR7R9LINYwouHIziqQYMAkGBYqGSM44BAMDLwawLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6R0k0k9K
-----END CERTIFICATE-----
```

5. Extraia o certificado do arquivo de certificado e armazene-o em uma variável chamada \$Store.

```
PS C:\> $Store =
[Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptography.X509Certificates.X509Certificate]::FromFile("certificate.pem"))
```

6. Verifique a assinatura.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

Se a assinatura for válida, o comando não retornará nenhuma saída. Se não for possível verificar a assinatura, o comando retornará `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer.` Se não for possível verificar a assinatura, entre em contato com o AWS Support.

7. Valide o conteúdo do documento de identidade da instância.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Se o conteúdo do documento de identidade da instância for válido, o comando retornará `True`. Se não for possível validar o documento de identidade da instância, entre em contato com o AWS Support.

Usar a assinatura codificada em base64 para verificar o documento de identidade da instância

Este tópico explica como verificar o documento de identidade da instância usando a assinatura codificada em base64 e o certificado público RSA da AWS.

Para validar o documento de identidade da instância usando a assinatura codificada em base64 e o certificado público RSA da AWS

1. Conecte-se à instância.
2. Recupere a assinatura codificada em base64 dos metadados da instância, converta-a em uma matriz de bytes e adicione-a à variável chamada `$Signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
PS C:\> $Token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância, converta-o em uma matriz de bytes e adicione-o a uma variável chamada `$Document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Adicione um dos seguintes certificados públicos RSA AWS a um novo arquivo chamado `certificate.pem`, dependendo da Região da sua instância.

Other AWS Regions

O certificado público da AWS a seguir se destina a todas as regiões da AWS, exceto Hong Kong, Bahrein, China e GovCloud.

```
-----BEGIN CERTIFICATE-----
```

```
MIIDIJCCAougjAwIBAgIJAknL4UEDMN/FMA0GCSqGSIB3DQEBBQUAMGoxCzAJBgNV
BAYTA1VTMRMwEQYDVQQIEwpXYXNoaW5ndG9uMRawDgYDVQQHEwdTZWF0dGx1MRgw
FgYDVQOKew9bbWF6b24uY29tIELuYy4xGjAYBGNVBAWEVjMi5hbWF6b25hd3Mu
Y29tMB4XDTE0MDYwNTE0MjgwMloXTD10MDYwNTE0MjgwM1owajELMAkGA1UEBhMC
VVMxEzARBgNVBAgTCldhc2hpmd0b24xKEDAOBgNVBAcTB1NLYXR0bGUxGDAWBgNV
BAoTD0FtYXpibi5jb20gsW5jLjEaMBgGA1UEAxMRZWMYlMftYXpvmF3cy5jb20w
gZ8wDQYJKoZIhvCNQEBBQADgY0AMIGJAOGBA1e9GN//SRK2knbjySG0ho3yqQM3
e2TdhwO8D2e8+XZqck754gFS99AbT2RmXClambI7xsYHZFapbELC4H91ycihvrD
jbST1ZjkLQggaONE1q43eS68ZeTDccScXQSNivS1zJZS8HJZjggzBlXjZftjtdJL
xeB4hwvo0s4f3j9AgMBAAGjgc8wgwwHQYDVROOBByEFCXWzAgVyrbwnFncFFIs
77Vbd1E4MIGCbgNVHSMEgZQwgZGAFCXWzAgVyrbwnFncFFIs77Vbd1E4oW6kbDBq
MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ1RvbjEQMA4GA1UEBxMHU2Vh
dHRszTEYMBYGA1UEChMPQW1hem9uLmNvbSBjbmMuMRowGAYDVQQDExFlyzIuYW1h
em9uYXdzLmNvbYIJAknL4UEDMN/FMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvCNQEF
BQADgYEAFYcz10gEhQBXIwIdsgCOS8vEtijYF+j9u06jz7V0mJqo+pR1AbR1vY8T
C1haGgSI/A1uZUKs/Zfnph0oEI0/hu1IIJ/SKBDtN51vmZ/IzbOPIJWirlsllQIO
7zvWbGd9c9+Rm3p04oTvhu991a7kZqevJk0QRdD/6NpCKsqP/0=
-----END CERTIFICATE-----
```

Hong Kong Region

O certificado público da AWS da região Hong Kong é o seguinte:

```
-----BEGIN CERTIFICATE-----
MIICzCCAbQCQDtQvkVxRvK9TANBqkqhkiG9w0BAQsFADBqM0swCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ1RvbjEQMA4GA1UEBxMHU2VhDHRszTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBjbmMuMRowGAYDVQQDExFlyzIuYW1hem9uYXdzLmNvbTAe
FwOxOTAyMDMwMzAwMDZaFw0yOTAYMDIwMzAwMDZaMGoxCzAJBgNVBAYTA1VTMRMw
EQYDVQOIEwpXYXNoaW5ndG9uMRawDgYDVQQHEwdTZWF0dGx1MRgwFgYDVQOKew9B
bWF6b24uY29tIELuYy4xGjAYBGNVBAWEVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIB3DQEBAQAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JhjTieHAgacaQkiR
Pity9QPDE3b+NxDh4Upd1xdIw73Jc1IG3sG9RhWiXVCCh6KkuCTqJfPUknIKk8vs
M3RXf1UpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIB3DQEBCwUA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydv32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOnQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI31P/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

Bahrain Region

O certificado público da AWS da região Bahrain é o seguinte:

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAM16uIV/zqjFMA0GCSqGSIB3DQEBCwUAMHIxCzAJBgNV
BAYTA1VTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRawDgYDVQQHAdTZWF0dGx1MSAw
HgYDVQOKDbBdbWF6b24gV2ViIFN1cnZpY2VzIExmQzEaMBgGA1UEAwRZWMYlMft
YXpvmF3cy5jb20wIBcNMtkwNDTQzjMjQ3WhgPMjE5ODA5MjKxNDMyNDdaMHIx
CzAJBgNVBAYTA1VTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRawDgYDVQQHAdTZWF0
dgx1MSAwHgYDVQOKDbBdbWF6b24gV2ViIFN1cnZpY2VzIExmQzEaMBgGA1UEAwR
ZWMYlMftYXpvmF3cy5jb20wgZ8wDQYJKoZIhvCNQEBBQADgY0AMIGJAOGBALVN
CDTzEnIeoX1SEYqq6k1BV0Z1pY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZrgGeRge1ePWD1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NN1+vynyioWUUrw7/wIZTAGMBAAGjgdccwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FoXakdDByM0swCQYDVQOGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhDHRszTEgMB4GA1UECgwxQW1hem9uIFd1YiBTZXJ2
aWN1cyBMTEMxGjAYBGNVBAWEVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhKNTB1FgWFd+ZhC/LhRUY
40jEiykmbEp6hlzQ79t0Tfbn5A4NYDI2icBP0+hmf6qSn1hwJF6typyd1yPK5Fqt
NTPxxcXmUKqux+pHmIkK1LKD08rNE84jqxrRsfdi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
```

-----END CERTIFICATE-----

Cape Town Region

O certificado público da AWS da região Cidade do Cabo é o seguinte:

```
-----BEGIN CERTIFICATE-----  
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIEExBXYYNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xOTEwMjcw  
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT  
EFdhc2hpemd0b24gU3RhGUxEDAOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft  
YXpbvIBXZWIGu2VydmljZXMGTExDMIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKB  
gQDFd571nUzVtke3rPyRkYFys3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F  
7TuB/ZEN+vmlYqr2+5Va8U8qlbPF0bRH+FdaKjhgWzdYxxGzQzU3i0y5W5ZM1VyB  
7iUsxEAlxsybC3ziPyAH42UiTkQnahmoroNeqVyhNnBpQIDAQABMA0GCSqGSIB3  
DQEBCwUAA4GBAAJLylWye1EqOpW4B1XPYRVD4pAds8Guw2+krgqkY0HxLCdjosuH  
RytGDGN+q75aaOxzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK  
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK  
-----END CERTIFICATE-----
```

Milan Region

O certificado público da AWS da região Milão é o seguinte:

```
-----BEGIN CERTIFICATE-----  
MIICNjCCAZ+gAwIBAgIJAOZ3GEIAcugMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIEExBXYYNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xOTEwMjQx  
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT  
EFdhc2hpemd0b24gU3RhGUxEDAOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft  
YXpbvIBXZWIGu2VydmljZXMGTExDMIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKB  
gQCjPgW3vsXRj4JoA16WDQDyoPc/eh3QBARaApJEC4nPIGUoUlpaXCjfhWplo2O+  
ivgfCsc4AU9OpYdAPha3spLey/bhPRi1JZHRNqScKPhzsCNmKhfnZTIEQCFvsp  
DRp4zr91/WS06/f1JFBYJ6JHhp0KwM81XQG591V6kk0W7QIDAQABMA0GCSqGSIB3  
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv  
XKRXL1KdM/dfiuYGokDGxiCOMg6TYy6wvR2qRhtXW1OtZkiHwcQCnOtz+8vpew  
wx8JGMvowtuKB1iMsbwypZkFYLcvh+Opfb/Aayi20/ChQldI6M2R5VU  
-----END CERTIFICATE-----
```

China Regions

O certificado público da AWS para as regiões China (Pequim) e China (Ningxia) é o seguinte.

```
-----BEGIN CERTIFICATE-----  
MIICSzCCAbQCCQCQ97teKRD4zANBgkqhkiG9w0BAQUFADBqMQswCQYDVQQGEwJV  
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBGA1UE  
ChMPQW1hem9uLmNvbSBjbMuMRowGAYDVQQDEXFlYzIuYW1hem9uYXdzLmNvbTAe  
Fw0xMzA4MjExMzIyNDNaFw0yMzA4MjExMzIyNDNaMGoxCzAJBgNVBAYTA1VTMRMw  
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGx1MRgwFgYDVQQKEw9B  
bWB6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G  
CSqGSIB3DQEBAQUAA4GNADCBiQKBgQC6GFQ2WoB11xZYH85INUMaTc4D30QXM6f+  
YmWzyJD9fc7ZOUlaZIKoQATqC058KNCre+jECELYIX56Uq01b8LRLP8tijrQ9Sp3  
qJcXiH66kH0eQ44a5YdewcFOy+CSAYDUiaB6XhTQJ2r7bdA2vv3ybbxTOWONkD0  
WtgIe3M3iwIDAQABMA0GCSqGSIB3DQEBBQUAA4GBAHzQC5XZVeD9GTJTsb05AyH  
ZQvki/jfARNrD9dgBRYZzLC/NOkWG6M9wlrnks9RtdNxc53nLxKq4I2Dd73gI0yQ  
wYu9YYwmM/LMqmPlI33Rg20hwq4DVgT3hO170PL6Fsgiq3dMvctsImJvjWktBQaT  
bcAgaZLHGIpXPrWSA2d+  
-----END CERTIFICATE-----
```

GovCloud Regions

O certificado público da AWS para as regiões GovCloud da AWS é o seguinte.

```
-----BEGIN CERTIFICATE-----  
MIIDCzCCAnSgAwIBAgIJAi...  
-----END CERTIFICATE-----
```

5. Verifique o documento de identidade da instância.

```
PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
```

Se a assinatura for válida, o comando retornará `True`. Se não for possível verificar a assinatura, entre em contato com o AWS Support.

Usar a assinatura RSA-2048 para verificar o documento de identidade da instância

Este tópico explica como verificar o documento de identidade da instância usando a assinatura RSA-2048 e o certificado público RSA-2048 da AWS.

Prerequisites

Este procedimento exige a classe `System.Security` Microsoft .NET Core. Para adicionar a classe à sessão do PowerShell, execute o comando a seguir.

```
PS C:\> Add-Type -AssemblyName System.Security
```

Note

O comando adiciona a classe somente à sessão atual do PowerShell. Se você iniciar uma nova sessão, deverá executar o comando novamente.

Como verificar o documento de identidade da instância usando a assinatura RSA-2048 e o certificado público RSA-2048 da AWS

1. Conecte-se à instância.
2. Recupere a assinatura RSA-2048 dos metadados da instância, converta-a em uma matriz de bytes e adicione-a a uma variável chamada `$Signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
PS C:\> $Token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/token).Content
```

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância, converta-o em uma matriz de bytes e adicione-o a uma variável chamada \$Document. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Crie um novo arquivo chamado certificate.pem e adicione um dos certificados públicos RSA-2048 da AWS a seguir, dependendo da Região.

North America Regions

- Norte da Virginia

```
-----BEGIN CERTIFICATE-----  
MIIEjCCAvggAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIEzM0zAgFw0xNTA4MTQw  
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT  
EFdhc2hpbmdb0b24gU3RhdGUxEAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FT  
YXpvbiBXZWIGu2VydmIjZXMGTExDMMIIBIjANBgkqhkiG9w0BAQEFAOCAQ8AMIIB  
CgKCAQEAs2vqZu9mEOhQg+0bRpAbCUiapbZMFNQgRg7kTlr7CF+gDqXKpHPjsng  
SfNz+JHqd8WP1+pmNs+qZ2aTe23klmf2U52KH9/jk18R1Ibap/yFibFTSedmegX  
E5r447GbJRSHUmuiIfZTz0rLpIo5/Vz7Soj22tdkdY2ADp7caZkNxhSP915fk  
2jJMTBUOzyXUS2rBU/u1NHbTTeepJjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h  
Um4cFApzzGn3aD5j2LrSMu2pctkQwf9CaWyVznqrsgYjYOY66LuFzSCXwqSnFBfv  
fFBAAfsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRAAsGA1UdDwOEAWIHgDAd  
BgNVHQ4EFgQUrynsPp4uqSECwy+Pi04gyJ8TWSkwgY4GA1UdIwSBhjCBg4AUryns  
Pp4uqSECwy+Pi04gyJ8TWSmhYKRewMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX  
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6  
b24gV2ViIFNlcnPzY2VzIEzM04IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C  
AQAwDQYJKoZIhvCNQELBQADggEBADW/s81Xi jwdP6NkEoH1m9XLrvk4YTqkNfR6  
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3tyOHkDk6SJMs85  
haoJNAFF7EQ/zCp1EJRikLLsC7bcDL/Eriivs78/BB4RnC9W9kSp/sxd5svJMg  
N9a6FAplpNRsWAmbP8JB1AP93oJzb1x2LQXgykTghMkQ07NaY5hg/H5o4dMPclTK  
1YGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
```

```
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOW09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

- Ohio

```
-----BEGIN CERTIFICATE-----
MIIIEjCCAvqqAwIBAgIJALM07oeX4xevdMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExMoZAgFw0xNja2MTAx
MjU4MTMhaGA8yMTk1MTEExNDEyNTgxOFowXDELMakGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmdb0b24gU3RhdGUxEDAObgNVBActB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlgU2Vydm1jZXMGTExDmIIBiIANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEA6v6kGMnRmFDLxEqXzP4npnL65000kmQ7w8YXQygSdmN1oScGSU5wf9
mZdcvCxCdxgALFsFqPvH8fq1E9ttI0fEf0zvHos8wUsIdKr0zz0MjSx3cik4tKET
ch0EkfMnzK0gDBavracDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAAm5oYMFpX6M6St77WdNE8wEU8SuerOughimVx9kMB07imeVHBiELbMQON
1wSWRL/61fA02keGSTfSp/0m3u+1esf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7Kt03HTG9i1XQIDAQAB04HUMIHRMAsGA1UdDwOEAWIHgDAd
BgNVHQ4EFgQU2CTGYE5ftJx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFN1cnZpY2VzIExMo4IJA07oeX4xevdMBlGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKz0IhvCNQELBQADggEBANdjkIpVyp2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtpQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
IBjcTFBBI1xBeFkZoO3wczo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdnB
n6FYnluIcDbmpcQePoVwqX7W3oOYLb1QLN7fe6H1j4TBIsFd03OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoK07Ilp0fOT6fz41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOfjrgDAb2ogbFy8LzHo2ztSe60M=
-----END CERTIFICATE-----
```

- Oregon

```
-----BEGIN CERTIFICATE-----
MIIIEjCCAvqqAwIBAgIJALZL31rQCSTMMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExMoZAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMakGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmdb0b24gU3RhdGUxEDAObgNVBActB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlgU2Vydm1jZXMGTExDmIIBiIANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMy9ALA/Ipz0n0Huxj38EBZmX/NdNqKm7C
qWu1q5kmIVYjKGiafdboU8wLchO8ywvfg16FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/iidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ej0ty4h7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3La13/+wIDAQAB04HUMIHRMAsGA1UdDwOEAWIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
-----END CERTIFICATE-----
```

- Norte da Califórnia

```
-----BEGIN CERTIFICATE-----
MIIIEjCCAvqqAwIBAgIJJANNPkIpCYEtIMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExMoZAgFw0xNTEwMjk
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMakGA1UEBhMCVVMxGTAXBgNVBAgT
-----END CERTIFICATE-----
```

```
EFdhc2hpbd0b24gU3RhdGUxEADOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlqU2VydmljZXMGTExdMIIBIjANBqkqhkiG9w0BAQEFAOCAQ8AMiIB
CgKCAQEApHQGvHvq3SVCzdrC7575BW7GWLzcj8CLqYcL3YY7JffupzOjcft057Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6Cd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KCh
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2ChkJsj
AIWwgopFpwH1jVYm7obmuIxSIUv+oNH0wXgDL029Zd98sNIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBqFcTtWPky+POGu81DYFqiWVEyR2JKkm2/iR1dL1YsT39kbNg47xY
ar129sS4nB5Vw3TRQa2jLOToTlxzhQIDAQABo4HUMIHRMAsGA1UdDwOEAWIHgDAd
BgNVHQ4EFgQUgepyiONs8+jq67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8+jq67dmcWu+mKKDa+ihYKReMFwxCzAJBqNVBAYTA1VTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnPzY2VzIExm04IJAANNPkiPcyEtIMBIGA1UdEWEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNQELBQADggEBAGLFWyutf1u0xCAC+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR81lcv8ZElXDb0NC6v8UeLpe1WBkjawQtEjl1ifKg9hdY9Rj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xehOAZEjAXzVvHp8Bne33VVwMiMxWECZCijxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2BzBti5eu7vMG4i3AYWuFVLthaBgu
1PfHafJpj/JDcq2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

- Canada (Central)

```
-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJAJNKhJhaJOUmMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgnV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExm0zAgFw0xNjA3MjKx
MTM3MTdaGA8yMTk2MDewMjExMzcxn1owXDELMakGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbd0b24gU3RhdGUxEADOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlqU2VydmljZXMGTExdMIIBIjANBqkqhkiG9w0BAQEFAOCAQ8AMiIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY819XoHndnxmP50Cqld
+26AJt1tlqHpi1Ydtz6OrvRgvHxVtbvte01z3ldEzC3PMvmISBhHs6A3SWHA91n
InBhToLX/SWqBHL0X78HkPRA2G2k0COHPry+fG9gvz8HCiQaXcbWNFDHZev90ToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUCMO0
LBvmTGGehWhi04MUZwfOkn9jjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUb17Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp81EoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVp112OgRWLcT
rJg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTp3FQThH010KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+tteHwRRngX7
-----END CERTIFICATE-----
```

South America Regions

- São Paulo

```
-----BEGIN CERTIFICATE-----
MIIIEjCCAvqgAwIBAgIJAMcyoxxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgnV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExm0zAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMakGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbd0b24gU3RhdGUxEADOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlqU2VydmljZXMGTExdMIIBIjANBqkqhkiG9w0BAQEFAOCAQ8AMiIB
CgKCAQEAv45lhGZvbQcy1fHBqzRoOh8Csrdzxj/WP4cRbjo/2DAnimvrCCDs5086
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPwC6EYYAnR+P1LG+aNSOGUzszy202S03hT0
B20hWPCqpPp39itRhG4id6nbNRjOzLm6evHuPMAHR4/OV7hyGoiGaV/v9zqiNA
pMCLhbh2xkP035HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTcfiqp0TjyRWapM29OhA
CRJfJ/d/+wBtZ1fkWOZ7TP+EWRIN5ITEad1DTPnF1r8kBruDcS/lIGFwrOOHLo4C
CKoNgXkhTqDDBDu6oNBb2rS0K+sZ3QIDAQABo4HUMIHRMAsGA1UdDwOEAWIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUgBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBqNVBAYTA1VTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6
-----END CERTIFICATE-----
```

```
b24gV2ViIFNlcnPzY2VzIEzM04IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNQELBQADggEBACoWSBF7b9A1cNr14l1r3QWWSc7k90/tUzal
P1T0G3Ob12x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGxbGSCJSEJkW
vGCtc/jYMHxFhx67Szmf7m/MTYVnvzsyoQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRoktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbhdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPfk3+107o910Vrhq1QRB0gr1Exrv1LbyfU=
-----END CERTIFICATE-----
```

Europe, Middle East, and Africa Regions

- Frankfurt

```
-----BEGIN CERTIFICATE-----
MIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQHEwdTZWF0
dGxlMSAwHgYDVQOKExdbBWF6b24gV2V1IFNlcnPzY2VzIEzM0zAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpmd0b24gU3RhdGUxEDAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2VydmljZXMGTExdMIIBiIANBgkqhkiG9w0BAQEFAOCaQ8AMIIB
CgKCAQEAKa8FLhxS1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6x8n/3o/+wt10Cn6MLsiUeHqN15H/4U/Q/FR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIBScrjR4V03TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/Sjp1vloxe2KuWnyC+EKIInka909s14ZAUh+qIYfZK85DAjm
GJP4W036E9wIJUQF2hZJrzs1B1MGYC1WI9veRISd30iZZL6VVXLXUthwVhnVASrS
zzDvPzj+3yD5hRxsvFigGhY0FCFVFnwIDAQAB04HUMIHRMASGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC216pvJaRflgu3MuDn6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC21
6pvJaRflgu3MuDn6zTuP6YehYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQOKExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQHEwdTZWF0dGxlMSAwHgYDVQOKExdbBWF6
b24gV2ViIFNlcnPzY2VzIEzM04IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNQELBQADggEBAlk+DtbUPpJXFqQMV1f2Gky5/82ZwgbffXa
HBeGSii55b3tsyC3ZW5z1MJ7DtNr3vUkiWbV1EUaZGOU1ndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xbf0mTKPrOGdvymjZUtQMSVb91bMWCfFs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgx01gWhKTnYbaZ0xkJvEvccKxVAwJ
obF8NyJla0/pWdjhlHafEXEN81yyxyTTyOa0BGTuYOBD2cTYyinauVKY4fqHUkr3v
Z6fboaHed4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

- Londres

```
-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJANBx0E2b0CEPMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQOKExdbBWF6b24gV2V1IFNlcnPzY2VzIEzM0zAgFw0xNjA4MTEx
dGxlMSAwHgYDVQOKExdbBWF6b24gV2V1IFNlcnPzY2VzIEzM0zAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpmd0b24gU3RhdGUxEDAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2VydmljZXMGTExdMIIBiIANBgkqhkiG9w0BAQEFAOCaQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzbWCjOwpsuHE9H6dWUUyl2Bgnu+z
d8QvW306Yleec45M4F2RA3J4hWhtShzsml0JVRT+yUlGetf90CPr26QmIFFs5nD4
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOpsCR+bHOu0Xykdk10MnIbpBf0kTfciaUpQEA
dEHnM2J1L2i0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdiwVQpdWkbDL9BCG1YjyadQjxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbrQIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQBG
wujwU1Otp13iBgmhjMC1gZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+sNaOEauOn2FF
aiYjvY0/hXQx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSpb0WRqTBxq5
Ed7F7+7GR1eBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/lpi
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDvb3IiH8kPR/J0Qn+hvO12HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbgwK
-----END CERTIFICATE-----
```

- Paris

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVmxGTAXBgNVBAgT
EFdhc2hpbmdb0b24gU3RhdGUxEADoBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlgu2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEaY5V7KDqnEvF3DrSProFCgu/oL+QYD62b1u+Nq8aPuljJe127Sm9WnWA
EBdOSASkOa9fzjCPoG5SGjWkxYoZjsevHpmzjVv9+Ci+F57bSuMbJgUbvbRIFUB
bxQojVoXQPHgk5V433ODxkQ4s+jRyUbf4YV1AFdfU7zabC698YgPV0EghXP1Tvco
8mlc631ubw2g52j0lzaozUkHPsbnTomhQIV06kUFx0e0tDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2U11DFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96i1vUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXCg+sVlcaQG9q59xC5z8HvJZ1+SxzPKKC4PKQdKvIIIfE8GxVXqlZG1
c15WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1H11XGjhx611CGcENH1egI31OTILsa
+KfopuJEQ9QTDMAIkGjhA+KieU/U5Ct9fdej6d0G6C0EuwKktTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQjCZ8jy1YcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiut5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJxaM
-----END CERTIFICATE-----
```

- Irlanda

```
-----BEGIN CERTIFICATE-----
MIIIEejCCAvggAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNTEwMjkw
OTA2MTlaGA8yMTk1MDQwMzA5MDYx0VowXDELMAkGA1UEBhMCVVmxGTAXBgNVBAgT
EFdhc2hpbmdb0b24gU3RhdGUxEADoBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlgu2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEaJEt7nVu+aHltzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCTc4ssnf
zQHq2JRVr0GRchvDrbmlHaP/avtfQR/Thvfltwu9AROVt22dUOTvERdkNzveoFCy
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCdfcChxRYZ6mP90+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ881
FI+qYKs7xsjQYgXWfEt6bckWsi1kZiaI0yMzYdPF6C1LyZee/UhIe/uJyUUNfpT
VIsIS01tBcPf4C7Y20j0IwWI2SgQOIDAQABo4HUMIHRMasGA1UdDwQEAWIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Z18mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUf2Dg
PUZivKQR/Z18mB/MxIkjZDUhgYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnPzY2VzIExMo4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNQELBQADggEBAGm6+57W5brzJ3+t8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1R1XTMYgXXx10YggX88XPmPtok17
14hib/D9/lu4IaFIyLzYNSzsETYKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTigoW41G58sfw5b+wjXCsh0nRoOn79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZikZqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREE4NoETf+Mu5G
4CqoaPR05KwdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

- Milão

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVmxGTAXBgNVBAgT
EFdhc2hpbmdb0b24gU3RhdGUxEADoBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlgu2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBq7sFGKPiwhkbpuB61rRxKHhj8V9vaReM
1nv1Ur5LAPpMPYDsuj4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/OipHh/X2hc2S9wvxKWiShu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XtgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qz1RTzLapXp4/5
iNwusrTNexG18BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
-----END CERTIFICATE-----
```

```
5ya11K/hKgvaRTvZwVV8G1VZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad51G4tEbtepX456XXc058MKmcnzNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjl57LHZICssD+XPifXay69OF1scIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvgIwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

- Estocolmo

```
-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJAJALc/uRxg++EnMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxM沃XDELMakGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpbmdb0b24gU3RhdGUxEAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpzbIBXZWlIgU2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAEzawCGJEJ1xqtr2FD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSAKavxwX3X6tJA8fveGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTuWOpJ1Cm3u9R/VzilCNwkj7iQ65AFA18Enmsw3UG1dEsop4
yChKB3KW3W10FTh0+gD0YtjrqqYxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GULFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGDsal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSib3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcdw+3y/F0fWz561YORhP2FnPoMekf0S1/
Jqk4svzJbCbQeMzRoyaya/46d7UiioXMHRZam5IaGBh0dQbi97R4VsQjwQj0RmQsq
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGf1K4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xz1DULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW6160MkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYeJBsdzKG4
FEyxIdEjoe01jhTsck3R
-----END CERTIFICATE-----
```

- Bahrein

```
-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpbmdb0b24gU3RhdGUxEAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpzbIBXZWlIgU2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAEy4VnIt2eBpEjKgOKBmyupJzJAI74fr74tueGJNwwa+Is2vH12jMzn9I11
UpvvEUYTIboIgISpf6S5Lm5rCv4jT4a1Wm0kjfNbiilkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpfd635JLU3K1BLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU119daQeG9roHR+4rIWSpaoopmMxv5nctgypOrE6zKxx2dNxQ1dd
VULV+WH7s6Vm4+yBeG8ctPYH5Goo+QIDAQABMA0GCSqGSib3DQEBCwUAA4IBAQBs
ZcViiZdFdpCXESZP/KmZNDxB/kkt1IEhsQ+Mnn29jayE5oLmtGjhj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYzxRF1VBuFA
WGZO+98kxCs4n6tTwVt+nsuJr9BjRVc17apfHBgSS8c50Wna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q341XZ629iyFirSJ5TTOic0osNL7vwM0Yj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBi6ZlqAoFlLrjGzxBPiwrRM/XrGmF8ze4KzoUqJEnK1306A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

- Cidade do Cabo

```
-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJAIFI+05A6/ZIMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNfowXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpbmdb0b24gU3RhdGUxEAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpzbIBXZWlIgU2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAEy7/WHBBH0rk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
-----END CERTIFICATE-----
```

```
oeVmR9nqnhfij2w0cQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkx02YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuCONRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctlQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Or7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoG1v5XbHJe2o
JFD8GRRy2rkWO/1NwVFDcwec6zC3QwIDAQABMA0GCSqGSIsb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBjsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoY2aaXU
VEB/oQziRGyKdN1d4TGyVZXG44CkrzSDvbmfiTq5tl+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEE6YYE1Rakl62VncYSxiGe/i2Xvs1NH3Olmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU81JgFEvPWMDFU5sGB6ZM
gkEKTzMv1ZpPbBhg99J1
-----END CERTIFICATE-----
```

Asia Pacific Regions

- Sydney

```
-----BEGIN CERTIFICATE-----
MIIIEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIsb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMakGA1UEBhMCVVMxGTAXBgnVBAGT
EFdhc2hpbmdb24gU3RhdGUxEDAObgNVBAcTB1N1YXR0bGUxIDAeBqNVBAoTFOFt
YXpvbiBXZWIGu2VydmljZXMGTExdMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAmRcyLwrayS8yDC1b5Abs3TUaJabjqwu7d5gHik5Icd6dk18EypQSeS
vz6pLhkgO4xRbCRGlgE8LS/OijcZ5HwdxRiKbicR1YvIPaIyEQQvF5sX6UwkGYw
Ma5IRGj4YbRmjKBybw+AAV9Icb5LJNOMWPi340WM+2tMh+8L234v/JA6ogpdPuDr
SM6YFHMZONw058MQ0FnEj2D7H58Ti//vFP10taaPWAIRF85zBiJtkCFJ6vPdqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAqWHj2AaQrGSCITxCM1s9sJ
151DeoZBjnx8cnRe+HcA4YoRBiqIQIDAQABo4HUMIHRMASGA1UdDwQEAwIHgDAD
BgNVHQ4EFgQU/wHIo+r5U31VisPoWoRvsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VisPoWoRvsNXGxoyhYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX
YXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnPzY2VzIExMQ4IJA1bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNQELBQADggEBACobLvj8Ix1QyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPefFTdBW9W3YCNc34Ss9TJq2D7t/zLGGlbi4wYXU6VYJjL0S
hCjWeIyBXUZOZKFCb0DSjeUElsTRSXFuVrZ9EawjLvhni3BaC9Ve34ip71ifr75
8Tpk6PEj0+jwiijFH8E4GhcV5chB0/iooU6i0QqJrMwFyNwo1cVZJD5v6D0mu9bS
TMIJLJKv4Q0QqPsNdjib7G9bfkB6trP8fUVYLHLsV1Iy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RIMNs/IMG7VmH1bf4swHOHBgCN1uYo=
-----END CERTIFICATE-----
```

- Tóquio

```
-----BEGIN CERTIFICATE-----
MIIIEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIsb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAYNVowXDELMakGA1UEBhMCVVMxGTAXBgnVBAGT
EFdhc2hpbmdb24gU3RhdGUxEDAObgNVBAcTB1N1YXR0bGUxIDAeBqNVBAoTFOFt
YXpvbiBXZWIGu2VydmljZXMGTExdMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEaz0djWUcmRW85C5CiCKPFiTIVj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gM1u+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+i
KeznOtxzqQ5w05NLE9bA61sziaUFNVstFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMLTeMNvPItKOC1eRL111SgXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F70Er7XqmNODOL6yh92Qz8fHjG+afOL9Y2Hc4g+P1nk4w4i0hQOPABqzb
MPjK7B2Rze0f90Ec51GBQu13kxkWWQIDAQABo4HUMIHRMASGA1UdDwQEAwIHgDAD
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fdwRihYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX
YXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnPzY2VzIExMQ4IJA1bFgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNQELBQADggEBAG/N7ua8IE9IMynoOn5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFFt0rLOKo54pJ+Kim2cngCWNhkcrtRHBV567AJNt4+ZDG5
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----  
MIID0zCCAiOgAwIBAgIJANuCgChtOjhMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNTA5MTQx  
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMakGA1UEBhMCVVMxGTAXBgNVBAgT  
EFdhc2hpbmdb24gU3RhdGUxEDAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbiBXZWIGu2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCAQ8AMIIB  
CgKCAQEA661Nv6pJPmGM20W8HbVVJS1KcAg2vUGx8xeAbZzIQdpGfkabVcUHGB6m  
Gy59VXDMlrlJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs  
m06QZqg5qKjBP6xr3+Pshf01rBmwg0gXEm22CC7077+7N7Mu2sWzWbiUR7vi14  
9FjWS8XmMnwFT1Shp411TDTevDWw/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa  
LHaVCH/Yy52rsz0hM/FlgmSnK105ZKj+b+Kip3adBL8OMCjgc/Pxi0+j3HQldYE  
32+FaxWU84D2iP2gDT28evnstuYTQIDAQABMA0GCSqGSib3DQEBCwUAA4IBAQc1  
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokXomwo8r  
KHbbqvtK8510xUzp/Cx4sm4aTgcMvfJP29jGLclDzeqADIVkWEJ4+xncxSYV1S9x  
+78TvF/+8h9U2LnS164PXaKdxHy2IshIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN  
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy81kiOsvU9XzUaZ0fZSfxx  
wXxZamQbONvFcXvHY/OPSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMr04  
jmKe0aMy3thyK6g5sJVg  
-----END CERTIFICATE-----
```

- Seul

```
-----BEGIN CERTIFICATE-----  
MIID0zCCAiOgAwIBAgIJANuCgChtOjhMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNTA3MTKx  
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMakGA1UEBhMCVVMxGTAXBgNVBAgT  
EFdhc2hpbmdb24gU3RhdGUxEDAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbiBXZWIGu2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCAQ8AMIIB  
CgKCAQEAzrnEYef8IjhrJoazi0QGZkm1mHm/4rEbYqbMNifxjsDE8WtHNwaM91z  
zmyK6Sk/tKLwxcn13g31iq305ziyFPEewe5Qbwfliz2cMsVfNBcTh/E6u+mBPH3J  
gvGanqUjt6c4IbipdEouIjjnyNyWd4D6erL1/ENijeR10xVpaqSW5SBK7jms49E  
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmk1cqTfMfPCkzmJCRgp  
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijedn7kTsQzg0072SAE63PI048JK8HcObH  
txORUQ/XF1jzi/SIAUJZT7kq3kWl8wIDAQABMA0GCSqGSib3DQEBCwUAA4IBAQbj  
Tht09dLvU20mKuXAhxXjsId1QgGG3ZGh/Vke4If1ymqLx95v2Vj9Moxk+gJuUSR  
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gi8kqkG7V8iRyPIFekv+M  
pcail+cIv5IV5qAz8QOMGYfGdykcoBjsgiyvMu/2N2UbZJNGWvcEGkdjGJUYYYOO  
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiiUgEaW3UFEbThJT+z8UFHG9fQjzzfN/J  
nt6vuY/ORRulxAZPyh2gr5okN/s6rnmh2zmBHUi1n8cbCc64MVfXe2g3EZ9Glq/9n  
izPrI09hMyjpDP04ugQc  
-----END CERTIFICATE-----
```

- Osaka

```
-----BEGIN CERTIFICATE-----  
MIID0zCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNzA3MTKx  
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMakGA1UEBhMCVVMxGTAXBgNVBAgT  
EFdhc2hpbmdb24gU3RhdGUxEDAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbiBXZWIGu2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCAQ8AMIIB  
CgKCAQEAzrnEYef8IjhrJoazi0QGZkm1mHm/4rEbYqbMNifxjsDE8WtHNwaM91z  
zmyK6Sk/tKLwxcn13g31iq305ziyFPEewe5Qbwfliz2cMsVfNBcTh/E6u+mBPH3J  
gvGanqUjt6c4IbipdEouIjjnyNyWd4D6erL1/ENijeR10xVpaqSW5SBK7jms49E  
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmk1cqTfMfPCkzmJCRgp  
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijedn7kTsQzg0072SAE63PI048JK8HcObH  
txORUQ/XF1jzi/SIAUJZT7kq3kWl8wIDAQABMA0GCSqGSib3DQEBCwUAA4IBAQbj  
Tht09dLvU20mKuXAhxXjsId1QgGG3ZGh/Vke4If1ymqLx95v2Vj9Moxk+gJuUSR  
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gi8kqkG7V8iRyPIFekv+M  
pcail+cIv5IV5qAz8QOMGYfGdykcoBjsgiyvMu/2N2UbZJNGWvcEGkdjGJUYYYOO  
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiiUgEaW3UFEbThJT+z8UFHG9fQjzzfN/J  
nt6vuY/ORRulxAZPyh2gr5okN/s6rnmh2zmBHUi1n8cbCc64MVfXe2g3EZ9Glq/9n  
izPrI09hMyjpDP04ugQc  
-----END CERTIFICATE-----
```

- Mumbai

```
-----BEGIN CERTIFICATE-----  
MIID0zCCAiOgAwIBAgIJAPRYyD8TtmCOMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNjAzMDcx  
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMakGA1UEBhMCVVMxGTAXBgNVBAgT  
EFdhc2hpbmdb24gU3RhdGUxEDAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbiBXZWIGu2VydmljZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCAQ8AMIIB  
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj  
07Xw7eENC+T79mOxAbewg91KaODOzw6i91/2/HpK0+NDEdD6sPKDA1d45jRra+v  
CqAjI+nV9Vw91wv7HJMk3RcjWGziM8/hw+3YNIutt7aqzZrwIWlBpcqrx3/AFd8Eu  
-----END CERTIFICATE-----
```

```
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+z
w9RVHm24BgH1LxLHLmsOIxvbrF277uX9dxu1HfKfu5D2kimTY7xS2DNLR2dt+kNY
/+iWdIeEFpPT0PLSILT52wP6stF+3QIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iy07Vkm1wkJiZsMhXpk73zxf
TPxuXEacTX3SOea07OIMCFwkus05f6leOyFTynHCzBz3U0ukRVZA3WcpbNB6Dwy
h7ysVlqyT9Wzd7EOYm5j5oue2G2xdei+6etgn5UjyWm6lizGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYEx/ZS6zEhd4CCDLgYkIjlrbFB3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2Cc1CHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

- Hong Kong

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgnVBAGt
EFdhc2hpbm0b24gU3RhdGUxEDA0BgvTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2VydmljZXmgTExDMiIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAA4T1PNSog0FDrg1WePoHeOsM0JTA3HCry5LsbyD33GFU2eBrOixoU/+SM
rInKu3GghAMFH7WxPW3etIAZiyTDDU5RLcUqzQwdr/zpXAWpYocNc/CEmBFfbxF
z4uwBIN3/dm0RSbe/wP9EcgmNUGQMMZWeAjisMtpOb1NWAP9Bn1UG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6048TR5yTaV+3Ran2SGRhjJfjh3FRpP4VC+z5LnT
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401Gsm9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQDK
2/+C3nPmgtYOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
1MzoQXjffkVZ97J7RNDW06oB7kj3WVE8a7U4WEOfn0/CbMuF/x99CckNDwpjgW+
K8V8SzAsQDVYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX-v/T1lc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXXUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3if8s81uTheiQjwY5t9nMoSY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJ1
tmmeJMJ7xeURdpBBx36Di
-----END CERTIFICATE-----
```

- Cingapura

```
-----BEGIN CERTIFICATE-----
MIIIEjCCAvvgAwIBAgIJAJVMGw5SHkcvcMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOvowXDELMAkGA1UEBhMCVVMxGTAXBgnVBAGt
EFdhc2hpbm0b24gU3RhdGUxEDA0BgvTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2VydmljZXmgTExDMiIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAA1aSSLfb17OgmikjLReHuNhVuvM20dCsVzpUyRbut+KmIEec24wd/xVy
2RMIRydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkyBdcYbe9o/0Q4P7IVS3
X1vwrUu0qo9nSID0mxMnOoF118KAQnn10tQ0W+1NSTkasW7QVzcb+3okPEvhPAoq
Mnly3vkM0GI8zx4iOKBEcSVIzf6wuIfXMGHVC/JjwhiJ2USQ8fq6oy686g54P4w
ROg415kLYCcodjqThmGJPNUpAZ7M0c5Z4pymfuChgNAZnvjhZDA8420jecqm62zcm
Tzh/pNMNeGCRYq2EQX0aqtYOIj7b0QIDAQABo4HUMIHRMAsGA1UdDwEAwIHgDAD
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnPzY2VzIExMQ4IJAJVMGw5SHkcvcMBIGA1UdEwEB/wQIMAYBAf8C
AQAWDQYJKoZIhvcaNQELBQADggEBAF/0dWqkIEZKg5rc8a0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEWjYeeV2kY63skJ+QpuYbSuIBLM8p/uTRIVyM4IZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhNw47iIOBiqSAUKIr3Y3BDaDn
EjeXF6qS4iPIVBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQ1RTTVKXFN7pCRUV
+L9FuQ9y8mP0BYza5e1sdkwebydu+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYyvi2961doRUyv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

- Ningxia

```
-----BEGIN CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3B1zcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMakGA1UEBhMCVVmxGTAXBgNVBAgT
EFdhc2hpbmdb24gU3RhdGUxEAOBgNVBAcTB1NLYXR0bGUxIDAeBgnVBAoTF0Ft
YXpvbiBXZWlgu2VydmljZXMGTExDmIIBiJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOIGi4A6+YTlzcDllyP8b8SCT2M/6PGKwzKJ5XbSB0L3gsnSwiFYqPg9c
uJPNb19wSA9vlyfWmd90qvTf1NrT6viewP813QdJ3EENzOx4ERcf/Wd22tV72kxD
yw1Q3I10MH4b0ItGQAxU50tXCjBZEEUZooOku8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc41ulsJqbN+5QW6fFrCNG/0Mr1b3JbwdfUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbent1qd7wvPJU556LZuhfqI0TohiIT1Ah+yUdN5osoamxTHKKtf/CsSJ1F
w3qXqFJQAOVWSqjFyHXFI1/GoupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQcN
Um00QHvUsJSN6KATbhgwLynHn3wZS0suS8EOCOpCFJFxP2SV0NYkERbxuOn/Vhi
yq5F8v4/bRA2/xpedLwmvFs7QW1omuXhSnYFkd33Z5gxnXPb9vRkLwiMSw4uXls35
qOraczUJ9EXDhrv7VmngIk9H3YssYr1DGeh/oz4Ze4UL0gnfkauanHikk+BUESg
/jSTD+7e+niEZJPihHdsVKFDlud5pkEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu616kfzigGkJBxkcq4gre3szZFdCQcUiobjZ4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

- Pequim

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAotrM5XLLSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMakGA1UEBhMCVVmxGTAXBgNVBAgT
EFdhc2hpbmdb24gU3RhdGUxEAOBgNVBAcTB1NLYXR0bGUxIDAeBgnVBAoTF0Ft
YXpvbiBXZWlgu2VydmljZXMGTExDmIIBiJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVbz+wQNdPiM9S+aUULOQEr1TmNDUrjLWlr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hiOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+ML1CN9TwRK0ToEabmDKorss4zFl7VSSbQJwcBSfOciwbdrRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9XssOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4Obx1FN92VtvzD6QBs3CcoFWgyWGvgzg+dNG5VcbsiiuRdimi3kciJz3H
Nv1wCczoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQa8
ezx5LRjzUU9EYWYhyYIEshF1P1qdhs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcR0115ag8d/JXGzcTCn1DXLxx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokE1otbH1P+g5y113b12leYE6Tm8
LKbyfK/532xJPq09abx4Ddn89ZEC6vvWVNDgTsxErg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

AWS GovCloud Regions

- Região GovCloud (Oeste dos EUA) da AWS

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMakGA1UEBhMCVVmxGTAXBgNVBAgT
EFdhc2hpbmdb24gU3RhdGUxEAOBgNVBAcTB1NLYXR0bGUxIDAeBgnVBAoTF0Ft
YXpvbiBXZWlgu2VydmljZXMGTExDmIIBiJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzICGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6XXXeFrCDAmOq0wUhi
3fRCuoeH1KOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
1W98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMIOY7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyh14f+pWaSOpQ01DpXvZAByvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQa/
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPk16DjdF9utqZ0JUo/Fxe1xm0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1pXD7wyRWuETmykk73uEyeWFByKCHwsO9sI+6204Vf8Jkuj/cie
-----END CERTIFICATE-----
```

```
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
71UX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WoWTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----
```

- AWSRegião GovCloud (Leste dos EUA) da

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxPhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIEzM0zAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVoWxDELMAkGA1UEBhMCVVmxGTAxgNVBAgT
EFdhc2hpmd0b24gU3RhdGUxEADOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlqU2VydmljZXMcTEXMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvax9sI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUDSVEuVrK3bLjaSsMOS7Uxmnn71YT9901ReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFj0xDqbNzkE1b1W7vK7ydsJTfMSl1jga54UAVXibQt9EAIf7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNEjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBT
hO2W/Lm+Nk0qxsXW6mqQFsAoucASC/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENS+
mKmYu11ZvhB0mLshyl1h3RRoL30hp3jCwXyt kWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpvcvmGH1OhMf3UzChMwbIr6udoD1MbSI07+8F+jUJkh4Xl11Kb
YeN5fsLZp7T/6YvbFSPPmbn1YoE2vKtuGKxObRrhU3h4JHdp1ZellpZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----
```

5. Extraia o certificado do arquivo de certificado e armazene-o em uma variável chamada \$Store.

```
PS C:\> $Store =
[Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptography.X509Certificates.X509Certificate]::FromFile("certificate.pem"))
```

6. Verifique a assinatura.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

Se a assinatura for válida, o comando não retornará nenhuma saída. Se não for possível verificar a assinatura, o comando retornará `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer.` Se não for possível verificar a assinatura, entre em contato com o AWS Support.

7. Valide o conteúdo do documento de identidade da instância.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Se o conteúdo do documento de identidade da instância for válido, o comando retornará `True`. Se não for possível validar o documento de identidade da instância, entre em contato com o AWS Support.

Melhores práticas e recomendações para o clustering do SQL Server no EC2

O clustering Always On oferece alta disponibilidade sem necessidade de armazenamento compartilhado. A lista de práticas neste tópico, além dos pré-requisitos definidos em [Pré-requisitos, restrições e recomendações para Grupos de disponibilidade AlwaysOn](#), pode ajudar você a obter os melhores resultados ao operar um cluster Always On do SQL Server na AWS. As práticas listadas nesse tópico também oferecem um método de reunir logs.

Note

Quando os nós forem implantados em zonas de disponibilidade diferentes, ou em sub-redes diferentes dentro da mesma zona, eles deverão ser tratados como um cluster de várias sub-redes. Tenha isso em mente ao aplicar as melhores práticas e ao resolver possíveis cenários de falha.

Tópicos

- [Atribuir endereços IP \(p. 670\)](#)
- [Propriedades do cluster \(p. 671\)](#)
- [Votos no quórum do cluster e divisões 50/50 em um cluster multissite \(p. 671\)](#)
- [Registro de DNS \(p. 671\)](#)
- [Elastic Network Adapters \(ENAs\) \(p. 672\)](#)
- [Clusters multissite e posicionamento da instância do EC2 \(p. 672\)](#)
- [Seleção do tipo de instância \(p. 672\)](#)
- [Atribuir interfaces de rede elástica e IPs à instância \(p. 672\)](#)
- [Rede do heartbeat \(p. 673\)](#)
- [Configurar o adaptador de rede no sistema operacional \(p. 673\)](#)
- [IPv6 \(p. 673\)](#)
- [TTL de registro do host para listeners do grupo de disponibilidade do SQL \(p. 673\)](#)
- [Logging \(p. 674\)](#)
- [NetBIOS sobre TCP \(p. 674\)](#)
- [NetFT Virtual Adapter \(p. 674\)](#)
- [Definir possíveis proprietários \(p. 674\)](#)
- [Ajustar os limites de failover \(p. 675\)](#)
- [Importância do Witness e arquitetura do quórum dinâmico \(p. 676\)](#)
- [Troubleshoot \(p. 676\)](#)

Atribuir endereços IP

Cada nó de cluster deve ter uma interface de rede elástica atribuída que inclua três endereços IP privados na sub-rede: um endereço IP primário, um endereço IP do cluster e um endereço IP do grupo de disponibilidade. O sistema operacional (SO) deve estar com a NIC configurada para DHCP. Ela não deve ser definida como endereço IP estático, pois os endereços IP do cluster e do grupo de disponibilidade serão gerenciados virtualmente no gerenciador de cluster de failover. A NIC pode ser configurada para um IP estático, desde que seja configurada para usar somente o IP primário do eth0. Se os outros IPs forem atribuídos à NIC, isso pode fazer com que a rede caia para a instância durante os eventos de failover.

Quando a rede cair porque os IPs foram atribuídos incorretamente, ou quando houver um evento de failover ou falha de rede, não é incomum ver as seguintes entradas no log de eventos no momento da falha.

```
Isatap interface isatap.{9468661C-0AEB-41BD-BB8C-1F85981D5482} is no longer active.
```

```
Isatap interface isatap.{9468661C-0AEB-41BD-BB8C-1F85981D5482} with address  
fe80::5efe:169.254.1.105 has been brought up.
```

Como essas mensagens parecem descrever os problemas de rede, é fácil confundir a causa da pane ou da falha como erro de rede. No entanto, esses erros descrevem um sintoma – não uma causa – da falha. ISATAP é uma tecnologia de encapsulamento que usa IPv6 sobre IPv4. Quando a conexão IPv4 falha, o adaptador ISATAP também falha. Quando os problemas de rede são resolvidos, essas entradas não deverão mais aparecer nos logs do evento. Você também pode eliminar os erros de rede ao desabilitar com segurança a ISATAP com o comando a seguir.

```
netsh int ipv6 isatap set state disabled
```

Ao executar esse comando, o adaptador será removido do gerenciador de dispositivos. Esse comando deve ser executado em todos os nós. Ele não afeta a capacidade de funcionamento do cluster. Em vez disso, quando o comando tiver sido executado, a ISATAP não será mais usada. No entanto, como esse comando pode causar impactos desconhecidos em outras aplicações que usam ISATAP, ele deve ser testado.

Propriedades do cluster

Para ver a configuração completa do cluster, execute o comando do PowerShell a seguir.

```
Get-Cluster | Format-List -Property *
```

Votos no quórum do cluster e divisões 50/50 em um cluster multissite

Para saber como funciona o quórum do cluster e o que esperar em caso de falha, consulte [Noções básicas sobre cluster e quórum de grupo](#).

Registro de DNS

No Windows Server 2012, o Failover Clustering, por padrão, tenta registrar cada nó do DNS sob o nome do cluster. Isso é aceitável para aplicações que sabem que o destino do SQL está configurado como vários sites. No entanto, quando o cliente não estiver configurado dessa forma, pode resultar em timeouts, atrasos e erros na aplicação em função das tentativas de conexão a cada nó individual e falhas nos nós inativos. Para evitar esses problemas, o parâmetro Cluster Resource (Recurso do cluster) RegisterAllProvidersIp deve ser alterado para 0. Para obter mais informações, consulte [RegisterAllProvidersIP Setting e Multi-subnet Clustered SQL + RegisterAllProvidersIP + SharePoint 2013](#).

O RegisterAllProvidersIp pode ser modificado com o script de PowerShell a seguir.

```
Import-Module FailoverClusters
$cluster = (Get-ClusterResource | where {($_.ResourceType -eq "Network Name") -and
    ($_.OwnerGroup -ne "Cluster Group")}).Name
Get-ClusterResource $cluster | Set-ClusterParameter RegisterAllProvidersIP 0
Get-ClusterResource $cluster | Set-ClusterParameter HostRecordTTL 300
Stop-ClusterResource $cluster
Start-ClusterResource $cluster
```

Além de definir o parâmetro Cluster Resource (Recurso do cluster) como 0, é necessário garantir que o cluster tenha permissões para modificar a entrada do DNS para o nome do seu cluster.

1. Faça login no Domain Controller (DC) para o domínio ou para um servidor que seja host da zona de forward lookup para o domínio.
2. Abra o console do DNS Management e localize o registro A para o cluster.
3. Clique com o botão direito do mouse sobre o registro A e selecione Properties (Propriedades).
4. Selecione Security (Segurança).
5. Escolha Adicionar.
6. Selecione Object Types... (Tipos de objeto...), escolha a caixa Computers (Computadores) e selecione OK.
7. Insira o nome do objeto de recurso do cluster e selecione Check name (Verificar nome) e OK if resolve (OK se resolver).
8. Marque a caixa de seleção Full Control (Controle total).
9. Escolha OK.

Elastic Network Adapters (ENAs)

A AWS identificou problemas conhecidos com algumas workloads de clustering executadas na versão 1.2.3 do driver ENA. Recomendamos fazer upgrade para a versão 1.5.0 ou posterior e ajustar as configurações da NIC no sistema operacional. Para as versões mais recentes, consulte [Versões de driver do Amazon ENA](#). A primeira configuração, aplicável a todos os sistemas, aumenta os buffers de recebimento, que pode ser feito com o seguinte comando do PowerShell de exemplo.

```
Set-NetAdapterAdvancedProperty -Name (Get-NetAdapter | Where-Object {$_._InterfaceDescription -like '*Elastic*'}).Name -DisplayName "Receive Buffers" -DisplayValue 8192
```

Para instâncias com mais de 16 vCPUs, recomendamos evitar que o RSS seja executado na CPU 0.

Execute o seguinte comando.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_._InterfaceDescription -like '*Elastic*'}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

Clusters multissite e posicionamento da instância do EC2

Cada cluster é considerado um [cluster multissite](#). O serviço EC2 não compartilha endereços IP virtualmente. Cada nó deve ser uma [sub-rede](#) única. Ainda que não seja obrigatório, recomendamos que cada nó também esteja em uma zona de disponibilidade exclusiva.

Seleção do tipo de instância

O tipo de instância recomendada para Windows Server Failover Clustering depende da workload. Para workloads de produção, recomendamos instâncias compatíveis com [Otimização para EBS \(p. 1440\)](#) e [Redes avançadas \(p. 1028\)](#).

Atribuir interfaces de rede elástica e IPs à instância

Cada nó em um cluster do EC2 deve ter somente uma interface de rede elástica anexada. A interface de rede deve ter um mínimo de dois endereços IP privados atribuídos. No entanto, para workloads que usam Availability Groups, como SQL Always On, é preciso incluir um endereço IP adicional para cada grupo de disponibilidade. O endereço IP primário é usado para acessar e gerenciar o servidor; o endereço IP

secundário é usado como endereço IP do cluster; e cada endereço IP adicional é atribuído aos grupos de disponibilidade, conforme necessário.

Rede do heartbeat

Algumas documentações da Microsoft recomendam o uso de uma [rede de heartbeat](#) dedicada. No entanto, essa recomendação não se aplica ao EC2. Com o EC2, embora seja possível atribuir e usar uma segunda interface de rede elástica para a rede do heartbeat, ela usa a mesma infraestrutura e compartilha largura de banda com a interface de rede primária. Assim, o tráfego dentro da infraestrutura não pode ser priorizado nem se beneficiar com uma interface de rede dedicada.

Configurar o adaptador de rede no sistema operacional

A NIC no sistema operacional pode continuar usando o DHCP, desde que os servidores DNS recuperados do conjunto de opções de DHCP permitam que os nós se resolvam entre si. Você pode definir o NIC para ser configurado estaticamente. Quando concluído, você configura manualmente somente o endereço IP primário para a interface de rede elástica. O Failover Clustering gerencia e atribui endereços IP adicionais, conforme o necessário.

Para todos os tipos de instância, é possível aumentar a unidade de transmissão máxima (MTU) para 9001 no adaptador de rede, para que os [frames jumbo](#) sejam compatíveis. Essa configuração reduz a fragmentação de pacotes sempre que houver compatibilidade com os frames jumbo. O exemplo a seguir mostra como usar o PowerShell para configurar frames jumbo para um adaptador de rede elástico.

```
Get-NetAdapter | Set-NetAdapterAdvancedProperty -DisplayName "MTU" -DisplayValue 9001
```

IPv6

A Microsoft não recomenda desabilitar o IPv6 em um cluster do Windows. Ainda que o Failover Clustering funcione em um ambiente somente com IPv4, a Microsoft testa clusters com o IPv6 habilitado. Consulte [Failover Clustering and IPv6 in Windows Server 2012 R2](#) for details.

TTL de registro do host para listeners do grupo de disponibilidade do SQL

Defina o TTL de registro do host para 300 segundos, em vez do padrão de 20 minutos (1200 segundos). Para comparabilidade com o cliente legado, defina `RegisterAllProvidersIP` como 0 para os listeners do grupo de disponibilidade de SQL. Isso não é obrigatório em todos os ambientes. Essas configurações são importantes, pois algumas aplicações clientes legado não podem usar o `MultiSubnetFailover` nas strings de conexão. Consulte [Configuração de HostRecordTTL](#) para obter mais informações. Ao alterar essas configurações, o recurso do cluster deverá ser reiniciado. O grupo do cluster para o listener é interrompido quando o recurso do cluster é reiniciado, portanto, ele deve ser iniciado. Se você não iniciar o grupo do cluster, o grupo de disponibilidade permanecerá offline no estado RESOLVING. A seguir estão exemplos de scripts do PowerShell para alterar as configurações de TTL e `RegisterAllProvidersIP`.

```
Get-ClusterResource yourListenerName | Set-ClusterParameter RegisterAllProvidersIP 0
```

```
Get-ClusterResource yourListenerName | Set-ClusterParameter HostRecordTTL 300
```

```
Stop-ClusterResource yourListenerName
```

```
Start-ClusterResource yourListenerName
```

```
Start-ClusterGroup yourListenerGroupName
```

Logging

O nível de log padrão para o log do cluster é 3. Para aumentar o detalhamento das informações do log, defina o nível do log como 5. Consulte [Set-ClusterLog](#) para obter mais informações sobre o cmdlet do PowerShell.

```
Set-ClusterLog -Level 5
```

NetBIOS sobre TCP

No Windows Server 2012 R2, você pode aumentar a velocidade do processo de failover ao desabilitar NetBIOS sobre TCP. Esse recurso foi removido do Windows Server 2016. Teste esse procedimento se estiver usando sistemas operacionais mais antigos no ambiente. Para obter mais informações, consulte [Speeding Up Failover Tips-n-Tricks](#). A seguir está um exemplo do comando PowerShell para desabilitar NetBIOS sobre TCP.

```
Get-ClusterResource "Cluster IP Address" | Set-ClusterParameter EnableNetBIOS 0
```

NetFT Virtual Adapter

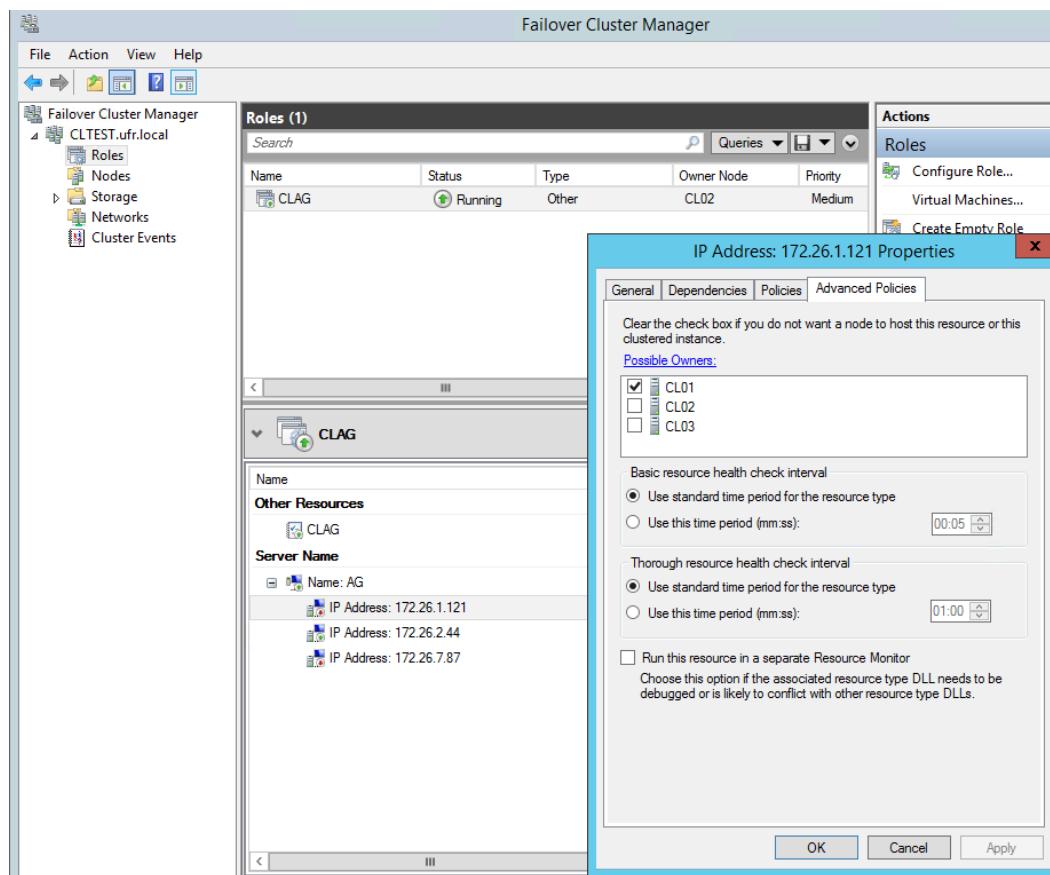
Para versões do Windows Server anteriores a 2016 e workloads não Hyper-V, a Microsoft recomenda habilitar o filtro de performance NetFT Virtual Adapter no adaptador do sistema operacional. Ao habilitar o NetFT Virtual Adapter, o tráfego interno do cluster é encaminhado diretamente para o NetFT Virtual Adapter. Para obter mais informações, consulte [NetFT Virtual Adapter Performance Filter](#). É possível habilitar o NetFT Virtual Adapter ao marcar a caixa de seleção nas propriedades da NIC ou usando o comando de PowerShell a seguir.

```
Get-NetAdapter | Set-NetAdapterBinding -ComponentID ms_netftf1t -Enable $true
```

Definir possíveis proprietários

O Gerenciador de cluster de failover pode ser configurado de forma que cada endereço IP especificado no painel Cluster Core Resources e nos recursos de grupo de disponibilidade possa ficar online somente no nó ao qual o IP pertence. Quando o gerenciador de cluster do failover não estiver configurado para isso e ocorrer uma falha, haverá certa demora no failover, pois o cluster tentará levantar os IPs nos nós que não reconhecem o endereço. Para obter mais informações, consulte [SQL Server Manages Preferred and Possible Owner Properties for AlwaysOn Availability Group/Role](#).

Cada recurso do cluster tem uma configuração para possíveis proprietários. Essa configuração explica ao cluster quais nós são permitidos para colocar um recurso online. Cada nó é executado em uma sub-rede única em uma VPC. Como o EC2 não pode compartilhar IPs entre instâncias, os recursos de IP no cluster podem ser colocados online somente por nós específicos. Por padrão, cada endereço IP que é adicionado ao cluster como recurso tem todos os nós listados como Possible Owner (Possível proprietário). Isso não resulta em falhas. No entanto, durante as falhas esperadas e inesperadas, você pode ver os erros nos logs sobre IPs em conflitos e falhas para levar os IPs online. Esses erros podem ser ignorados. Se você definir a propriedade Possible Owner (Possível proprietário), poderá eliminar esses erros totalmente, além de evitar o tempo ocioso enquanto os serviços são movidos para outro nó.



Ajustar os limites de failover

No Server 2012 R2, os limites de rede para a rede do heartbeat de failover usa como padrão valores altos. Consulte [Tuning Failover Cluster Network Thresholds](#) para ver mais detalhes. Essa configuração potencialmente não confiável (para clusters com alguma distância entre eles) foi resolvida no Server 2016 com um aumento no número de heartbeats. Descobriu-se que os clusters apresentam failover por conta de breves problemas transitórios de rede. A rede de heartbeat é mantida com UDP 3343, tradicionalmente muito menos confiável que TCP e mais propensa a conversas incompletas. Embora existam conexões de baixa latência entre as zonas de disponibilidade da AWS, ainda existem separações geográficas com diversos "hops" separando os recursos. Em uma zona de disponibilidade, pode haver uma distância entre os clusters, a menos que o cliente esteja usando placement groups ou hosts dedicados. Como consequência, há uma maior possibilidade de falha do heartbeat com UDP que com heartbeats baseados em TCP.

O único momento em que o cluster deve apresentar failover é quando houver uma pane legítima, como um serviço ou nó que apresenta um failover rígido, ao contrário de alguns pacotes UDP perdidos em trânsito. Para garantir que a pane é legítima, recomendamos ajustar os limites para atingirem, ou até mesmo superarem, as configurações para o Server 2016, conforme listado em [Tuning Failover Cluster Network Thresholds](#). Você pode alterar as configurações com os comandos PowerShell a seguir.

```
(get-cluster).SameSubnetThreshold = 10
```

```
(get-cluster).CrossSubnetThreshold = 20
```

Ao definir esses valores, os failovers inesperados devem ser drasticamente reduzidos. É possível ajustar essas configurações aumentando os atrasos entre heartbeats. Contudo, recomendamos enviar os heartbeats com mais frequência no caso de limites maiores. Definir esses limites ainda maiores garantem que os failovers só ocorram com situações de failover rígido, com atrasos mais longos antes de o failover ocorrer. Decida quanto tempo é aceitável para suas aplicações.

Depois de aumentar o `SameSubnetThreshold` ou o `CrossSubnetThreshold`, recomendamos aumentar o `RouteHistoryLength` para duplicar o mais alto dos dois valores. Isso garante que haja logs suficientes para a solução de problemas. Defina o `RouteHistoryLength` com o seguinte comando do PowerShell.

```
(Get-Cluster).RouteHistoryLength = 20
```

Importância do Witness e arquitetura do quórum dinâmico

Existe uma diferença entre Disk Witness (witness de disco) e File Share Witness (witness de compartilhamento de arquivo). O Disk Witness mantém um backup do banco de dados do cluster, enquanto o File Share Witness não faz isso. Os dois adicionam um [voto ao cluster \(p. 671\)](#). É possível usar o Disk Witness se você usar armazenamento baseado em iSCSI. Para obter mais informações sobre as opções de witness, consulte [Witness de compartilhamento de arquivo vs Witness de disco para clusters locais](#).

Troubleshoot

Se você enfrentar failovers inesperados, primeiro verifique se não está enfrentando problemas de rede, serviço ou infraestrutura.

1. Verifique se seus nós não estão passando por problemas de rede.
2. Verifique updates do driver. Se você estiver usando drivers desatualizados na sua instância, atualize-os. Atualizar seus drivers pode resolver problemas de erros e estabilidade que podem estar presentes na versão instalada atualmente.
3. Verifique se existem possíveis gargalos de recursos que estejam impedindo a instância de responder, como CPU e E/S de disco. Se o nó não conseguir atender as solicitações, pode parecer que ele foi desativado pelo serviço do cluster.

Atualizar uma instância do Amazon EC2 do Windows para uma versão mais recente do Windows Server.

Há dois métodos para atualizar uma versão anterior do Windows Server em execução em uma instância: atualização local e migração (também denominada atualização lado a lado). Uma atualização local atualiza os arquivos do sistema operacional, enquanto as configurações e os arquivos pessoais ficam intactos. A migração envolve a captura de configurações, as configurações, os dados e a portabilidade dos mesmos para um sistema operacional mais recente em uma nova instância do Amazon EC2.

A Microsoft recomenda tradicionalmente a migração para uma versão mais recente do Windows Server em vez de atualizá-lo. A migração pode resultar em menos erros ou problemas de atualização, mas pode demorar mais do que uma atualização local devido à necessidade de provisionar uma nova instância, planejar e fazer a portabilidade de aplicações e ajustar as configurações na nova instância. Uma atualização local pode ser mais rápida, mas incompatibilidades de software podem produzir erros.

Tópicos

- [Realizar uma atualização no local \(p. 677\)](#)
- [Realizar uma atualização automatizada \(p. 681\)](#)
- [Migrar para tipos de instância da geração mais recente \(p. 688\)](#)
- [Assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server \(p. 694\)](#)
- [Soluçinar problemas de uma atualização \(p. 702\)](#)

Realizar uma atualização no local

Para executar uma atualização local, você deve determinar quais drivers de rede a instância está executando. Os drivers de rede PV permitem que você acesse sua instância usando o Desktop Remoto. A partir do Windows Server 2008 R2, as instâncias usam AWS PV, adaptador de rede Intel ou os drivers de rede avançada. As instâncias com Windows Server 2003 e Windows Server 2008 usam drivers Citrix PV. Para obter mais informações, consulte [Drivers paravirtuais para as instâncias do Windows \(p. 559\)](#).

Atualizações automatizadas

Para ver as etapas de como usar o AWS Systems Manager para automatizar a atualização do Windows Server 2008 R2 para Server 2012 R2 ou de SQL Server 2008 R2 no Windows Server 2012 R2 para SQL Server 2016, consulte [Como atualizar suas workloads do Microsoft 2008 cujo suporte será encerrado na AWS com facilidade](#).

Antes de iniciar uma atualização no local

Execute as seguintes tarefas e observe os seguintes detalhes importantes antes de começar a atualização local.

- Leia a documentação da Microsoft para compreender os requisitos de atualização, os problemas conhecidos e as restrições. Além disso, leia as instruções oficiais de atualização.
 - [Atualização do Windows Server 2008 R2](#)
 - [Opções de atualização para Windows Server 2012](#)
 - [Opções de atualização para Windows Server 2012 R2](#)
 - [Opções de atualização e conversão para Windows Server 2016](#)
 - [Opções de atualização e conversão para Windows Server 2019](#)
 - [Centro de Atualização do Windows Server](#)
- Recomendamos a execução de uma atualização do sistema operacional em instâncias com pelo menos 2 vCPUs e 4 GB de RAM. Se necessário, você pode alterar a instância para um tamanho maior do mesmo tipo (t2.small para t2.large, por exemplo), executar a atualização e redimensioná-la de volta para o tamanho original. Se você precisar manter o tamanho da instância, poderá monitorar o progresso usando o [instance console screenshot \(p. 1581\)](#). Para obter mais informações, consulte [Alterar o tipo de instância \(p. 244\)](#).
- Verifique se o volume raiz de sua instância Windows tem espaço em disco suficiente. O processo de configuração do Windows poderá não avisá-lo sobre espaço em disco insuficiente. Para obter informações sobre a quantidade de espaço em disco que é necessária para atualizar um sistema operacional específico, consulte a documentação da Microsoft. Se o volume não tiver espaço suficiente, é possível expandi-lo. Para obter mais informações, consulte [Volumes elásticos do Amazon EBS \(p. 1409\)](#).
- Determine seu caminho de atualização. Você deve atualizar o sistema operacional para a mesma arquitetura. Por exemplo, você deve atualizar um sistema de 32 bits para um sistema de 32 bits. O Windows Server 2008 R2 e posterior são apenas 64 bits.
- Desabilite o software antivírus e antispyware e os firewalls. Esses tipos de software podem entrar em conflito com o processo de atualização. Habilite novamente o software antivírus e antispyware e os firewalls quando a atualização for concluída.

- Atualize para os drivers mais recentes, conforme descrito em [Migrar para tipos de instância da geração mais recente \(p. 688\)](#).
- O Upgrade Helper Service só oferece suporte a instâncias que estejam executando drivers Citrix PV. Se a instância estiver executando drivers Red Hat, atualize manualmente [esses drivers \(p. 565\)](#) primeiro.

Atualizar uma instância no local com AWS PV, adaptador de rede Intel ou drivers de rede avançada

Use o seguinte procedimento para atualizar uma instância do Windows Server usando AWS PV, adaptador de rede Intel ou drivers de rede avançada.

Para executar a atualização local

1. Crie uma AMI do sistema que você planeja atualizar para fins de backup ou teste. Em seguida, você pode fazer a atualização na cópia a fim de simular um ambiente de teste. Se a atualização for concluída, você poderá alternar o tráfego para essa instância com um período de inatividade curto. Se ocorrer falha na atualização, você poderá reverter para o backup. Para obter mais informações, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#).
2. Verifique se a instância do Windows Server está usando os drivers de rede mais recentes. Consulte [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#) para obter informações sobre como atualizar o driver AWS PV.
3. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
4. No painel de navegação, escolha Instances (Instâncias). Localize a instância. Anote o ID da instância e o ID da zona de disponibilidade da instância. Você precisará dessas informações mais tarde neste procedimento.
5. Se você estiver atualizando o Windows Server 2012 ou 2012 R2 para o Windows Server 2016 ou 2019, faça o seguinte na instância antes de continuar:
 - a. Desinstale o serviço EC2Config. Para obter mais informações, consulte [Interromper, reiniciar, excluir ou desinstalar o EC2Config \(p. 533\)](#).
 - b. Instale o serviço EC2Launch. Para obter mais informações, consulte [Instalar a versão mais recente do EC2Launch \(p. 523\)](#).
 - c. Instalar o SSM Agent do AWS Systems Manager. Para obter mais informações, consulte [Working with SSM Agent \(Trabalhar com o agente do SSM\)](#) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).
6. Crie um novo volume de um snapshot de mídia de instalação do Windows Server.
 - a. No painel de navegação à esquerda, em Elastic Block Store, escolha Snapshots. Na barra Filter (Filtro), escolha Public Snapshots (Snapshots públicos).
 - b. Adicione o filtro Owner (Proprietário) à barra de pesquisa e escolha Amazon images (Imagens da Amazon).
 - c. Adicione o filtro Description (Descrição) e insira **Windows**. Selecione Enter.
 - d. Selecione o snapshot que corresponde à arquitetura do sistema e à preferência de idioma para as quais você está fazendo a atualização. Por exemplo, selecione Windows 2019 English Installation Media para fazer a atualização para o Windows Server 2019.
 - e. Escolha Ações, Criar volume.
 - f. Na caixa de diálogo Create Volume (Criar volume), escolha a zona de disponibilidade que corresponde à instância do Windows e escolha Create Volume (Criar volume).
7. Na mensagem Volume Successfully Created (Volume criado com êxito), escolha o volume que você acabou de criar.
8. Escolha Ações, Anexar volume.

9. Na caixa de diálogo Attach Volume (Anexar volume), insira o ID da instância do Windows e escolha Attach (Anexar).
10. Torne o novo volume disponível para uso seguindo as etapas em [Make na Amazon EBS volume available for use on Windows \(Disponibilizar um volume do Amazon EBS para uso no Windows\)](#).

Important

Não inicialize o disco porque isso excluirá os dados existentes.

11. No Windows PowerShell, mude para a nova unidade de volume. Comece a atualização abrindo o volume de mídia de instalação que você anexou à instância.

- a. Se você estiver fazendo a atualização para o Windows Server 2016 ou posterior, execute o seguinte:

```
./setup.exe /auto upgrade
```

Se você estiver fazendo a atualização para uma versão anterior do Windows Server, execute o seguinte:

```
Sources/setup.exe
```

- b. Em Select the operating system you want to install, selecione o SKU de instalação completa da instância do Windows Server e escolha Next.
- c. Em Which type of installation do you want? (Qual tipo de instalação deseja?), escolha Upgrade (Atualizar).
- d. Assista todo o assistente.

A configuração do Windows Server copia e processa os arquivos. Após alguns minutos, sua sessão do Remote Desktop será encerrada. O tempo necessário para concluir a atualização depende do número de aplicações e das funções de servidor em execução na instância do Windows Server. O processo de atualização pode levar 40 minutos ou várias horas. A instância apresentará falha nas verificações de status 1 e 2 durante o processo de atualização. Quando a atualização for concluída, as duas verificações de status ocorrerão com êxito. Você pode verificar no log do sistema a saída do console ou usar as métricas do Amazon CloudWatch para a atividade do disco e da CPU a fim de determinar se a atualização está em andamento.

Note

Se você estiver fazendo a atualização para o Windows Server 2019, depois que a atualização for concluída, você poderá alterar a tela de fundo do desktop manualmente para remover o nome do sistema operacional anterior, se desejado.

Se a instância não passou nas duas verificações de status após várias horas, consulte [Solucionar problemas de uma atualização \(p. 702\)](#).

Atualizar uma instância no local com drivers Citrix PV

Os drivers Citrix PV são usados no Windows Server 2003 e 2008. Há um problema conhecido durante o processo de atualização em que a configuração do Windows remove partes dos drivers Citrix PV que permitem a conexão com a instância usando o Desktop Remoto. Para evitar esse problema, o procedimento a seguir descreve como usar o Upgrade Helper Service durante sua atualização no local.

Usar o Upgrade Helper Service

Você deve executar o Upgrade Helper Service antes de iniciar a atualização. Após a execução, o utilitário cria um serviço do Windows que é executado durante as etapas de pós-atualização para corrigir o estado do driver. O executável é gravado em C# e pode ser executado no .NET Framework versões 2.0 a 4.0.

Quando você executa o Upgrade Helper Service no sistema antes da atualização, ele executa as seguintes tarefas:

- Cria um novo serviço do Windows nomeado `UpgradeHelperService`.
- Verifica se os drivers Citrix PV estão instalados.
- Verifica a existência de drivers críticos de inicialização sem assinatura e exibe um aviso se algum for localizado. Os drivers críticos de inicialização sem assinatura poderão causar a falha do sistema após a atualização se os drivers não forem compatíveis com a versão mais recente do Windows Server.

Quando você executa o Upgrade Helper Service no sistema depois da atualização, ele executa as seguintes tarefas:

- Habilita a chave de Registro `RealTimeIsUniversal` para corrigir a sincronização de hora.
- Restaura o driver PV ausente executando o seguinte comando:

```
pnputil -i -a "C:\Program Files (x86)\Citrix\XenTools\*.inf"
```

- Instala o dispositivo ausente executando o seguinte comando:

```
C:\Temp\EC2DriverUtils.exe install "C:\Program Files (x86)\Citrix\XenTools\xevtchn.inf"
ROOT\XENEVTCHN
```

- Remove automaticamente o `UpgradeHelperService` ao concluir.

Executar a atualização em instâncias que executam drivers do Citrix PV

Para concluir a atualização, você deve anexar o volume de mídia de instalação à sua instância do EC2 e usar o `UpgradeHelperService.exe`.

Para atualizar uma instância Windows Server que executa drivers Citrix PV

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances e localize a instância. Anote o ID da instância e o ID da zona de disponibilidade da instância. Você precisará dessas informações mais tarde neste procedimento.
3. Crie um novo volume de um snapshot de mídia de instalação do Windows Server.
 - a. No painel de navegação, escolha Snapshotse, ao lado do campo de filtro, selecione Public Snapshots (Snapshots públicos).
 - b. Adicione o filtro Owner e escolha Amazon images.
 - c. Adicione o filtro Description (Descrição) e insira **Windows**. Pressione Enter.
 - d. Selecione o snapshot que corresponde à arquitetura do sistema de sua instância. Por exemplo, Windows 2012 Installation Media (Mídia de instalação do Windows 2012).
 - e. Escolha Ações, Criar volume.
 - f. Na caixa de diálogo Create Volume, selecione a zona de disponibilidade que corresponde à sua instância do Windows e escolha Create.
4. Na caixa de diálogo Volume Successfully Created, escolha o volume que você acabou de criar.
5. Escolha Ações, Anexar volume.
6. Na caixa de diálogo Attach Volume (Anexar volume), insira o ID da instância e escolha Attach (Anexar).
7. Em sua instância Windows, na unidade C:\, crie uma pasta denominada `temp`.

Important

Essa pasta deve estar disponível no mesmo local após a atualização. A criação da pasta em uma pasta do sistema do Windows ou em uma pasta de perfil de usuário, como o desktop, pode causar falha na atualização.

8. Faça download do [OSUpgrade.zip](#) e extraia os arquivos para a pasta C:\temp.
9. Execute C:\temp\UpgradeHelperService.exe e revise o arquivo C:\temp\Log.txt para ver se há avisos.
10. Use o [artigo da Base de conhecimento 950376](#) da Microsoft para desinstalar o PowerShell de uma instância Windows 2003.
11. Comece a atualização usando o Windows Explorer para abrir o volume de mídia de instalação que você anexou à instância.
12. Execute o arquivo Sources\Setup.exe.
13. Em Selecionar o sistema operacional que você deseja instalar, selecione o SKU de instalação completa para sua instância Windows Server e escolha Avançar.
14. Em Which type of installation do you want? (Qual tipo de instalação deseja?), escolha Upgrade (Atualizar).
15. Assista todo o assistente.

A configuração do Windows Server copia e processa os arquivos. Após alguns minutos, sua sessão do Remote Desktop será encerrada. O tempo necessário para concluir a atualização depende do número de aplicações e das funções de servidor em execução na instância do Windows Server. O processo de atualização pode levar 40 minutos ou várias horas. A instância apresentará falha nas verificações de status 1 e 2 durante o processo de atualização. Quando a atualização for concluída, as duas verificações de status ocorrerão com êxito. Você pode verificar no log do sistema a saída do console ou usar as métricas do Amazon CloudWatch para a atividade do disco e da CPU a fim de determinar se a atualização está em andamento.

Tarefas de pós-atualização

1. Inicie a sessão na instância para iniciar uma atualização do .NET Framework e reiniciar o sistema quando solicitado.
2. Instale a versão mais recente do serviço EC2Config (Windows 2012 R2 e anteriores) ou EC2Launch (Windows 2016 e posteriores). Para obter mais informações, consulte [Instalar a versão mais recente do EC2Config \(p. 532\)](#) ou [Instalar a versão mais recente do EC2Launch \(p. 523\)](#).
3. Instale o hotfix da Microsoft [KB2800213](#).
4. Instale o hotfix da Microsoft [KB2922223](#).
5. Se você fez a atualização para o Windows Server 2012 R2, recomendamos atualizar os drivers PV para drivers AWS PV. Caso tenha atualizado em uma instância baseada em Nitro, recomendamos a instalação ou atualização dos drivers NVME e ENA. Para obter mais informações, consulte [Windows Server 2012 R2 Instalar ou atualizar drivers AWS NVMe \(p. 580\)](#) ou [Como habilitar a rede avançada no Windows](#).
6. Habilite novamente o software antivírus e antispyware e os firewalls.

Realizar uma atualização automatizada

É possível executar uma atualização automatizada nas instâncias do Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 e SQL Server 2008 R2 com Service Pack 3 na AWS com documentos de automação do AWS Systems Manager.

Os documentos de automação do Systems Manager fornecem dois caminhos de atualização:

- Windows Server 2008 R2, 2012 R2 ou 2016 para Windows Server 2012 R2, 2016 ou 2019 usando o documento do Systems Manager para automação chamado [AWSEC2-CloneInstanceAndUpgradeWindows](#)
- SQL Server 2008 R2 no Windows Server 2012 R2 para SQL Server 2016 usando o documento do Systems Manager para automação chamado [AWSEC2-CloneInstanceAndUpgradeSQLServer](#)

Tópicos

- [Serviços relacionados \(p. 682\)](#)
- [Prerequisites \(p. 682\)](#)
- [Caminhos de atualização \(p. 684\)](#)
- [Etapas para executar uma atualização automatizada \(p. 685\)](#)

Serviços relacionados

Os seguintes serviços da AWS são usados no processo de atualização automatizada:

- AWS Systems Manager. O AWS Systems Manager é uma interface poderosa e unificada para gerenciar centralmente seus recursos da AWS. Para obter mais informações, consulte o [Guia do usuário do AWS Systems Manager](#).
- O AWS Systems Manager Agent (SSM Agent) é um software da Amazon que pode ser instalado e configurado em uma instância do Amazon EC2, em um servidor local ou em uma máquina virtual (VM). O SSM Agent permite que o Systems Manager atualize, gerencie e configure esses recursos. O agente processa as solicitações do serviço do Systems Manager na Nuvem AWS e as executa conforme especificado na solicitação. Para obter mais informações, consulte [Working with SSM Agent \(Trabalhar com o agente do SSM\)](#) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).
- AWS Systems Manager Documentos do SSM do. Um documento do SSM define as ações que o Systems Manager realiza nas suas instâncias gerenciadas. Os documentos do SSM usam JSON (JavaScript Object Notation) ou YAML e incluem etapas e parâmetros especificados por você. Esse tópico usa dois documentos SSM do Systems Manager para automação. Para obter mais informações, consulte [AWS Systems Manager Documents \(Documentos do AWS Systems Manager\)](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

Prerequisites

Para automatizar a atualização com documentos de automação do AWS Systems Manager, é necessário executar as seguintes tarefas:

- [Criar uma função do IAM com as políticas do IAM especificadas \(p. 682\)](#) para permitir que o Systems Manager execute tarefas de automação nas suas instâncias do Amazon EC2 e verifique se você atende aos pré-requisitos para usar o Systems Manager.
- [Selecione a opção de como você deseja que a automação seja executada \(p. 683\)](#). As opções para execução são Simple execution (Execução simples), Rate control (Controle de taxa), Multi-account and Region (Várias contas e região) e Manual execution (Execução manual).

Criar uma função do IAM com permissões especificadas

Para saber como criar uma função do IAM para permitir que o AWS Systems Manager acesse recursos em seu nome, consulte [Creating a Role to Delegate Permissions to an AWS Service \(Criar uma função para delegar permissões a um produto da AWS\)](#) no IAM User Guide (Manual do usuário do IAM). Este

tópico também contém informações sobre como verificar se sua conta atende aos pré-requisitos para usar o Systems Manager.

Selecionar a opção de execução

Ao selecionar Automation (Automação) no console do Systems Manager, selecione Execute (Executar). Depois de selecionar um documento de automação, você será solicitado a escolher uma opção de execução da automação. É possível escolher entre as opções a seguir. Nas etapas dos caminhos fornecidos neste tópico, usamos a opção Simple execution (Execução simples).

Execução simples

Escolha esta opção se deseja atualizar uma única instância, mas não deseja passar por cada etapa de automação para auditar os resultados. Tal opção é explicada com mais detalhes nas etapas de atualização a seguir.

Rate control (Controle de taxa)

Escolha esta opção se você deseja aplicar a atualização a mais de uma instância. Defina as configurações a seguir.

- Parâmetro

Essa configuração, que também é definida nas configurações Multi-Account and Region (Várias contas e região), define como sua automação se expande.

- Destinos

Selecione o destino ao qual você deseja aplicar a automação. Essa configuração também é definida nas configurações Multi-Account and Region (Várias contas e região).

- Valores de parâmetros

Use os valores definidos nos parâmetros do documento de automação.

- Grupo de recursos

Na AWS, um recurso é uma entidade com a qual você pode trabalhar. Os exemplos incluem instâncias do Amazon EC2, pilhas do AWS CloudFormation ou buckets do Amazon S3. Se você trabalha com vários recursos, pode ser útil gerenciá-los como um grupo, em vez de migrar de um serviço da AWS para outro em todas as tarefas. Em alguns casos, você pode querer gerenciar um grande número de recursos relacionados, como instâncias do EC2 que compõem uma camada de aplicação. Nesse caso, você provavelmente precisará realizar ações em massa nesses recursos ao mesmo tempo.

- Tags

As tags ajudam a categorizar os recursos da AWS de diferentes maneiras, como por finalidade, por proprietário ou por ambiente. Essa categorização é útil quando você tem muitos recursos do mesmo tipo. Você pode identificar rapidamente um recurso específico usando as tags atribuídas.

- Rate Control (Controle de taxa)

A opção Rate Control (Controle de taxa) também é definida nas configurações Multi-Account and Region (Várias contas e região). Ao definir os parâmetros de controle de taxa, você define a quanto da sua frota a automação será aplicada, seja por contagem de alvos ou por porcentagem da frota.

Multi-Account and Region (Várias contas e região)

Além dos parâmetros especificados em Rate Control (Controle de taxa), que também são usados nas configurações Multi-Account and Region (Várias contas e região), há duas configurações adicionais:

- Contas e unidades organizacionais (UOs)

Especifique várias contas nas quais você deseja executar a automação.

- AWS Regiões de

Especifique várias regiões da AWS nas quais você deseja executar a automação.

Execução manual

Esta opção é semelhante a Simple execution (Execução simples), mas permite percorrer cada etapa de automação e auditar os resultados.

Caminhos de atualização

Existem dois caminhos de atualização, que usam dois documentos de automação diferentes do AWS Systems Manager.

- [AWSEC2-CloneInstanceAndUpgradeWindows](#). Esse script cria uma imagem de máquina da Amazon (AMI) usando uma instância do Windows Server 2008 R2, 2012 R2 ou 2016 na conta e atualiza essa AMI para uma versão compatível de sua escolha (Windows Server 2012 R2, 2016 ou 2019). Esse processo com diversas etapas pode levar até duas horas para ser concluído.

Para atualizar a instância do Windows Server 2008 R2 para o Windows Server 2016 ou 2019, uma atualização no local é realizada duas vezes, primeiro do Windows Server 2008 R2 para o Windows Server 2012 R2 e, depois, do Windows Server 2012 R2 para o Windows Server 2016 ou 2019. A atualização direta do Windows Server 2008 R2 para o Windows Server 2016 ou 2019 não é compatível.

Nesse fluxo de trabalho, a automação cria uma AMI da instância e inicia a nova AMI na sub-rede que você fornecer. O fluxo de trabalho de automação executa uma atualização no local do Windows Server 2008 R2, 2012 R2 ou 2016 para a versão selecionada (Windows Server 2012 R2, 2016 ou 2019). Também atualiza ou instala os drivers da AWS exigidos pela instância atualizada. Após a conclusão da atualização, o fluxo de trabalho cria uma nova AMI e encerra a instância atualizada. Se você atualizar do Windows Server 2008 R2 para o Windows Server 2016 ou 2019, a automação criará duas AMIs, pois a atualização no local é realizada duas vezes.

- [AWSEC2-CloneInstanceAndUpgradeSQLServer](#). Este script cria uma AMI de uma instância do Amazon EC2 executando o SQL Server 2008 R2 SP3 em sua conta e atualiza a AMI para o SQL Server 2016 SP2. Esse processo com diversas etapas pode levar até duas horas para ser concluído.

Nesse fluxo de trabalho, a automação cria uma AMI da instância e inicia a nova AMI na sub-rede que você fornecer. A automação, então, executa uma atualização local do SQL Server 2008 R2 para o SQL Server 2016 SP2. Após a conclusão da atualização, a automação cria uma nova AMI antes de encerrar a instância atualizada.

Existem duas AMIs incluídas no processo de atualização automatizada:

- Instância atual em execução. A primeira AMI é a instância em execução atual, que não é atualizada. Essa AMI é usada para iniciar outra instância para executar a atualização no local. Quando o processo é concluído, essa AMI é excluída da sua conta, a menos que você solicite especificamente que a instância original seja mantida. Essa configuração é tratada pelo parâmetro `KeepPreUpgradeImageBackup` (o valor padrão é `false`, o que significa que a AMI é excluída por padrão).
- AMI atualizada. Esta AMI é o resultado do processo de automação. A segunda AMI inclui o SQL Server 2016 SP2 em vez do SQL Server 2008 R2.

O resultado final é uma AMI, que é a instância atualizada da AMI.

Quando a atualização estiver concluída, você poderá testar a funcionalidade do sua aplicação iniciando a nova AMI na VPC. Depois de concluir o teste e antes de executar outra atualização, programe o tempo de inatividade da aplicação antes de mudar completamente para a instância atualizada.

Etapas para executar uma atualização automatizada

Caminhos de atualização

- [Atualizar o Windows Server 2008 R2, 2012 R2 ou 2016 para o Windows Server 2012 R2, 2016 ou 2019](#) (p. 685)
- [Atualizar o SQL Server 2008 R2 para o SQL Server 2016](#) (p. 686)

Atualizar o Windows Server 2008 R2, 2012 R2 ou 2016 para o Windows Server 2012 R2, 2016 ou 2019

Esse caminho de atualização requer pré-requisitos adicionais para funcionar com sucesso. Esses pré-requisitos podem ser encontrados nos detalhes do documento de automação para [AWSEC2-CloneInstanceAndUpgradeWindows](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

Após a verificação das tarefas de pré-requisito adicionais, siga estas etapas para atualizar sua instância do Windows 2008 R2 para o Windows 2012 R2 usando o documento de automação no AWS Systems Manager.

1. Abra o Systems Manager no AWS Management Console (Console de Gerenciamento da AWS).
2. No painel de navegação à esquerda, escolha Automation (Automação).
3. Escolha Execute automation.
4. Procure o documento de automação chamado [AWSEC2-CloneInstanceAndUpgradeWindows](#).
5. Quando o nome do documento aparecer, selecione-o. Ao selecioná-lo, os detalhes do documento aparecerão.
6. Selecione Next (Próximo) para introduzir os parâmetros desse documento. Deixe Simple execution (Execução simples) selecionada na parte superior da página.
7. Insira os parâmetros solicitados com base na orientação a seguir.

- `InstanceId`

Tipo: string

(Obrigatório) A instância que executa o Windows Server 2008 R2, 2012 R2 ou 2016 com o SSM Agent instalado.

- `InstanceProfile`.

Tipo: string

(Obrigatório) O perfil da instância do IAM. Essa é a função do IAM usada para executar a automação do Systems Manager em relação à instância do Amazon EC2 e às AMIs da AWS. Para obter mais informações, consulte [Create an IAM Instance Profile for Systems Manager](#) (Criar um perfil de instância para o Systems Manager) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).

- `TargetWindowsVersion`

Tipo: string

(Obrigatório) Selecione a versão de destino do Windows.

- `SubnetId`

Tipo: string

(Obrigatório) Esta é a sub-rede do processo de atualização e onde reside sua instância de origem do EC2. Verifique se a sub-rede tem conectividade de saída para serviços da AWS, incluindo o Amazon S3 e também para a Microsoft (para fazer download de patches).

- `KeepPreUpgradedBackup`

Tipo: string

(Opcional) Se esse parâmetro estiver definido como `true`, a automação retém a imagem criada a partir da instância. A configuração padrão é `false`.

- `RebootInstanceBeforeTakingImage`

Tipo: string

(Opcional) O padrão é `false` (sem reinicialização). Se esse parâmetro estiver configurado como `true`, o Systems Manager reinicializará a instância antes de criar uma AMI para a atualização.

8. Depois de inserir os parâmetros, selecione Execute (Executar). Quando a automação começar, você poderá monitorar o progresso da execução.
9. Quando a automação for concluída, você verá o ID da AMI. Você pode iniciar a AMI para verificar se o sistema operacional Windows está atualizado.

Note

Não é necessário que a automação execute todas as etapas. As etapas são condicionais com base no comportamento da automação e da instância. O Systems Manager pode pular algumas etapas que não são obrigatórias.

Além disso, algumas etapas podem expirar. O Systems Manager tenta atualizar e instalar todos os patches mais recentes. Às vezes, porém, os patches expiram com base em uma configuração de tempo limite definida para a etapa especificada. Quando isso acontece, a automação do Systems Manager segue para a próxima etapa para garantir que o sistema operacional interno seja atualizado para a versão do Windows Server de destino.

10. Após a conclusão da automação, você pode iniciar uma instância do Amazon EC2 usando o ID da AMI para revisar sua atualização. Para obter mais informações sobre como criar uma instância do Amazon EC2 a partir de uma AMI da AWS, consulte [Como faço para iniciar uma instância do EC2 a partir de uma imagem de máquina da Amazon \(AMI\) personalizada?](#)

Atualizar o SQL Server 2008 R2 para o SQL Server 2016

Esse caminho de atualização requer pré-requisitos adicionais para funcionar com sucesso. Esses pré-requisitos podem ser encontrados nos detalhes do documento de automação para [AWSEC2-CloneInstanceAndUpgradeSQLServer](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

Após a verificação das tarefas de pré-requisito adicionais, siga estas etapas para atualizar o mecanismo de banco de dados do SQL Server 2008 R2 para o SQL Server 2016 usando o documento de automação no AWS Systems Manager.

1. Se isso ainda não foi feito, faça download do arquivo .iso do SQL Server 2016 e monte-o no servidor de origem.
2. Após a montagem do arquivo .iso, copie todos os arquivos do componente e coloque-os em qualquer volume de sua escolha.
3. Faça um snapshot do volume do EBS e copie o ID do snapshot em uma área de transferência para uso posterior. Para obter mais informações sobre como criar um snapshot do EBS, consulte [Como criar um snapshot do EBS](#) no Guia do usuário do Amazon Elastic Compute Cloud.
4. Anexe o perfil da instância à instância de origem do EC2. Isso permite que o Systems Manager se comunique com a instância do EC2 e execute comandos nele depois que ele é adicionado ao serviço

do AWS Systems Manager. Para esse exemplo, nomeamos a função `SSM-EC2-Profile-Role` com a política `AmazonSSMManagedInstanceCore` anexada à função. Para obter mais informações, consulte [Create an IAM Profile for Systems Manager \(Criar um perfil de instância do IAM para o Systems Manager\)](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

5. No console do AWS Systems Manager, no painel de navegação à esquerda, selecione Managed Instances (Instâncias gerenciadas). Verifique se sua instância do EC2 está na lista de instâncias gerenciadas. Se você não vir a instância depois de alguns minutos, leia [Where Are My Instances? \(Onde estão minhas instâncias?\)](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).
6. No painel de navegação à esquerda, escolha Automation (Automação).
7. Escolha Execute automation.
8. Escolha o botão ao lado do documento do SSM `AWSEC2-CloneInstanceAndUpgradeSQLServer` e selecione Next (Avançar).
9. Verifique se a opção Simple execution (Execução simples) está selecionada.
10. Insira os parâmetros solicitados com base na orientação a seguir.

- `InstanceId`

Tipo: string

(Obrigatório) A instância executando o SQL Server 2008 R2 (ou posterior).

- `IamInstanceProfile`

Tipo: string

(Obrigatório) O perfil da instância do IAM.

- `SnapshotId`

Tipo: string

(Obrigatório) O ID do snapshot para a mídia de instalação do SQL Server 2016.

- `SubnetId`

Tipo: string

(Obrigatório) Esta é a sub-rede do processo de atualização e onde reside sua instância de origem do EC2. Verifique se a sub-rede tem conectividade de saída para serviços da AWS, incluindo o Amazon S3 e também para a Microsoft (para fazer download de patches).

- `KeepPreUpgradedBackUp`

Tipo: string

(Opcional) Se esse parâmetro estiver definido como `true`, a automação retém a imagem criada a partir da instância. A configuração padrão é `false`.

- `RebootInstanceBeforeTakingImage`

Tipo: string

(Opcional) O padrão é `false` (sem reinicialização). Se esse parâmetro estiver configurado como `true`, o Systems Manager reinicializará a instância antes de criar uma AMI para a atualização.

11. Depois de inserir os parâmetros, selecione Execute (Executar). Quando a automação começar, você poderá monitorar o progresso da execução.
12. Quando Execution status (Status de execução) mostrar Success (Sucesso), expanda Outputs (Saídas) para exibir as informações da AMI. Você pode usar o ID da AMI para iniciar sua instância do SQL Server 2016 para a VPC de sua escolha.

13. Abra o console do EC2. No painel de navegação à esquerda, selecione AMIs. Você deve ver a nova AMI.
14. Para verificar se o SQL Server 2016 foi instalado com sucesso, selecione a nova AMI e escolha Launch (Executar).
15. Escolha o tipo de instância que você deseja para a AMI, a VPC e a sub-rede que você deseja implantar e o armazenamento que deseja usar. Como você está lançando a nova instância de uma AMI, os volumes são apresentados como uma opção para incluir na nova instância do EC2 que você está executando. Você pode remover qualquer um desses volumes ou adicionar volumes.
16. Adicione uma tag para ajudar você a identificar sua instância.
17. Adicione o grupo de segurança ou grupos à instância.
18. Escolha Launch Instance (Executar instância).
19. Escolha o nome da tag para a instância e selecione Connect (Conectar) no menu suspenso Actions (Ações).
20. Verifique se o SQL Server 2016 é o novo mecanismo de banco de dados na nova instância.

Migrar para tipos de instância da geração mais recente

As AMIs do Windows da AWS são configuradas com as definições padrão usadas pela mídia de instalação da Microsoft com algumas personalizações. As personalizações incluem drivers e configurações compatíveis com os tipos de instância de última geração, que são instâncias criadas no [Sistema Nitro \(p. 154\)](#), como M5 ou C5.

Ao migrar para as instâncias [baseadas em Nitro \(p. 154\)](#), inclusive instâncias bare metal, recomendamos seguir as etapas deste tópico nos seguintes casos:

- Se você estiver iniciando instâncias a partir de AMIs personalizadas do Windows
- Se você estiver iniciando instâncias a partir de AMIs do Windows fornecidas pela Amazon que foram criadas antes de agosto de 2018

Para obter mais informações, consulte [Atualização do Amazon EC2 – tipos de instância adicionais, Sistema Nitro e opções de CPU](#).

Note

Os procedimentos de migração a seguir podem ser executados no Windows Server versão 2008 R2 e posterior.

Sumário

- [Parte 1: Instalar e atualizar drivers da AWS PV \(p. 689\)](#)
- [Parte 2: Instalar e atualizar ENA \(p. 690\)](#)
- [Parte 3: Atualizar drivers AWS NVMe \(p. 690\)](#)
- [Parte 4: Atualizar o EC2Config e o EC2Launch \(p. 691\)](#)
- [Parte 5: Instalar o driver de porta serial para instâncias bare metal \(p. 692\)](#)
- [Parte 6: Atualizar as configurações de gerenciamento de energia \(p. 692\)](#)
- [Parte 7: Atualizar drivers do chipset Intel para novos tipos de instância \(p. 692\)](#)
- [\(Alternativa\) Atualizar os drivers PV, ENA e NVMe da AWS usando o AWS Systems Manager \(p. 693\)](#)

- Migrar para tipos de instância Xen a partir de tipos de instância Nitro (p. 694)

Note

Como alternativa, você pode usar o documento de automação do [AWS Support - UpgradeWindowsAWSDrivers](#) para automatizar os procedimentos descritos em Parte 1, Parte 2 e Parte 3. Se você optar por usar o procedimento automatizado, consulte [\(Alternativa\) Atualizar os drivers PV, ENA e NVMe da AWS usando o AWS Systems Manager \(p. 693\)](#) e continue com a Parte 4 e a Parte 5.

Antes de começar

Este procedimento supõe que você está em execução, atualmente, em uma geração prévia do tipo de instância baseada em Xen, como um M4 ou C4, e você está migrando para uma instância baseada no [Sistema Nitro \(p. 154\)](#), como um M5 ou C5.

Você deve usar a versão 3.0 do PowerShell, ou posterior, para fazer a atualização com êxito.

Note

Ao migrar para a última geração de instâncias, as configurações de IP estático ou de DNS personalizado na ENI existente poderão ser perdidas uma vez que a instância será padronizada para um novo dispositivo de adaptador de redes avançadas.

Antes de seguir as etapas neste procedimento, recomendamos que você crie um backup de instância. No [Console EC2](#), escolha a instância que requer a migração, abra o menu de contexto (botão direito do mouse), escolha Estado da instância e Parar.

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para preservar dados em volumes de armazenamento de instâncias, faça backup dos dados no armazenamento persistente.

Abra o menu de contexto (clique com o botão direito do mouse) da instância, no [Console EC2](#), escolha Imagem, e depois escolha Criar imagem.

Note

As partes 4 e 5 dessas instruções podem ser concluídas depois de migrar ou alterar o tipo de instância a geração mais recente, como M5 ou C5. Contudo, recomendamos que você os conclua antes de migrar, se você estiver migrando especificamente para um tipo de instância Bare Metal EC2.

Parte 1: Instalar e atualizar drivers da AWS PV

Embora os drivers AWS PV não sejam utilizados no sistema Nitro, você ainda deve atualizá-los se você estiver em versões anteriores do Citrix PV ou AWS PV. Os drivers AWS PV mais recentes resolvem erros em versões anteriores dos drivers que podem aparecer enquanto você estiver no sistema Nitro, ou se você precisar migrar de volta a uma instância baseada em Xen. Como prática recomendada, recomendamos sempre atualizar os drivers mais recentes de instâncias Windows na AWS.

Use o seguinte procedimento para executar uma atualização no local dos drivers AWS PV ou fazer uma atualização de drivers Citrix PV para drivers AWS PV no Windows Server 2008 R2, no Windows Server 2012, no Windows Server 2012 R2, no Windows Server 2016 ou no Windows Server 2019. Para obter mais informações, consulte [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#).

Para atualizar um controlador de domínio, consulte [Atualizar um controlador de domínio \(atualização do AWS PV\) \(p. 567\)](#).

Para executar uma atualização de drivers AWS PV

1. Conecte-se à instância usando o Remote Desktop e prepare a instância a ser atualizada. Desative todos os discos que não sejam do sistema antes de executar a atualização. Essa etapa não será necessária se você executar uma atualização no local dos drivers AWS PV. Defina serviços não essenciais como inicialização Manual no console de Services.
2. [Faça download](#) do pacote de drivers mais recente na instância.
3. Extraia o conteúdo da pasta e execute `AWSVPDriverSetup.msi`.

Depois de executar o MSI, a instância é reinicializada automaticamente e, em seguida, atualiza o driver. A instância pode ficar indisponível por até 15 minutos.

Após o término da atualização e a instância passar nas duas verificações de integridade no console do Amazon EC2, conecte-se à instância usando o Remote Desktop e verifique se o novo driver foi instalado. Em Device Manager (Gerenciador de dispositivos), em Storage Controllers (Controladores de armazenamento), localize AWS PV Storage Host Adapter (Adaptador host de armazenamento do AWS PV). Verifique se a versão do driver é a mesma que a versão mais recente listada na tabela Histórico de versões do driver. Para obter mais informações, consulte [AWSHistórico do pacote de drivers PV \(p. 561\)](#).

Parte 2: Instalar e atualizar ENA

Atualize para o driver Elastic Network Adapter mais recente para garantir todos os recursos de rede sejam suportados. Se você executou a instância e ela não tiver a rede avançada habilitada, faça download e instale o driver do adaptador de rede obrigatório na instância. Depois, defina o atributo da instância enaSupport para ativar a rede avançada. Você somente poderá ativar esse atributo em tipos de instância suportados e somente se o driver ENA estiver instalado. Para obter mais informações, consulte [Habilitar redes avançadas com o Elastic Network Adapter \(ENA\) em instâncias do Windows \(p. 1029\)](#).

1. [Faça download](#) do driver mais recente para a instância.
2. Extraia o arquivo zip.
3. Instale o driver executando o script de PowerShell `install.ps1` da pasta extraída.

Note

Para evitar erros de instalação, execute o script `install.ps1` como um administrador.

4. Verifique se AMI tem enaSupport ativado. Em caso negativo, continue seguindo a documentação em [Habilitar redes avançadas com o Elastic Network Adapter \(ENA\) em instâncias do Windows \(p. 1029\)](#).

Parte 3: Atualizar drivers AWS NVMe

Os drivers AWS NVMe são usados para interagir com volumes de armazenamento de instâncias de Amazon EBS e de SSD que são expostos como dispositivos de bloco de NVMe em sistema Nitro para melhor performance.

Important

As seguintes instruções são alteradas especificamente para quando você instala ou atualiza AWS NVMe em uma instância anterior de geração com a intenção para migrar a instância para o tipo de instância de geração mais recente.

1. [Faça download](#) do pacote de drivers mais recente na instância.
2. Extraia o arquivo zip.

3. Instale o driver executando `dpinst.exe`.
4. Abra uma sessão do PowerShell e execute este comando:

```
start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

Note

Para aplicar o comando, é necessário executar a sessão do PowerShell como administrador. As versões do PowerShell (x86) resultarão em um erro.

Esse comando executa somente um sysprep em dispositivos do driver. Não executa uma preparação de sysprep completa.

5. Para o Windows Server 2008 R2 e o Windows Server 2012, feche a instância, altere o tipo para uma instância de última geração e inicie-a, depois, prossiga para a Parte 4. Se você iniciar a instância novamente em um tipo de instância de geração anterior antes de migrar para um tipo de instância mais recente, ele não será reiniciado. Para outras AMIs do Windows compatíveis, você pode alterar o tipo de instância a qualquer momento após o sysprep do dispositivo.

Parte 4: Atualizar o EC2Config e o EC2Launch

Para instâncias do Windows, os utilitários EC2Config e EC2Launch mais recentes fornecem funcionalidade e informações adicionais na execução em sistema Nitro, incluindo o Bare Metal EC2. Por padrão, o serviço EC2Config está incluído em AMIs anteriores ao Windows Server 2016. O EC2Launch substitui o EC2Config nas AMIs do Windows Server 2016 e posterior.

Quando os serviços EC2Config e EC2Launch forem atualizados, as novas AMIs do Windows da AWS incluirão a versão mais recente do serviço. Contudo, você precisa atualizar suas próprias instâncias e AMIs do Windows com a versão mais recente do EC2Config e EC2Launch.

Para instalar ou atualizar EC2Config

1. Faça download e descompacte o [instalador do EC2Config](#).
2. Executar `EC2Install.exe`. Para uma lista completa de opções, execute `EC2Install` com a opção `/?`. Por padrão, a configuração exibe os prompts. Para executar o comando sem prompts, use a opção `/quiet`.

Para obter mais informações, consulte [Instalar a versão mais recente do EC2Config \(p. 532\)](#).

Para instalar ou atualizar EC2Launch

1. Se você já tiver instalado e configurado o EC2Launch em uma instância, faça um backup do arquivo de configuração do EC2Launch. O processo de instalação não preserva as alterações feitas nesse arquivo. Por padrão, o arquivo está localizado no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Faça download do `EC2-Windows-Launch.zip` em um diretório na instância.
3. Faça download do `install.ps1` no mesmo diretório onde você baixou o `EC2-Windows-Launch.zip`.
4. Executar `install.ps1`.

Note

Para evitar erros de instalação, execute o script `install.ps1` como um administrador.

5. Se você fez um backup do arquivo de configuração do EC2Launch, copie-o no diretório `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Para obter mais informações, consulte [Configurar uma instância do Windows usando o EC2Launch \(p. 522\)](#).

Parte 5: Instalar o driver de porta serial para instâncias bare metal

O tipo de instância `i3.metal` usa um dispositivo serial baseado em PCI em vez de um dispositivo serial baseado em porta de E/S. Os AMIs do Windows mais recentes automaticamente usam dispositivo de série baseado em PCI e tem o driver de porta serial instalados. Se você não estiver usando uma instância lançada de um AMI do Windows fornecido pela Amazon, datado de 11.04.2018 ou posterior, deverá instalar o Driver de porta serial para habilitar o dispositivo serial para recursos de EC2 como Geração de senha e Saída de console. Os utilitários EC2Config e EC2Launch mais recentes também suportam o `i3.metal` e fornecem funcionalidade adicional. Caso ainda não tenha feito, siga as etapas da Parte 4.

Para instalar o driver de porta serial

1. [Faça download](#) do pacote de drivers de série mais recente na instância.
2. Extraia o conteúdo da pasta, abra o menu de contexto (clique com o botão direito) em `aws_ser.INF` e selecione install (instalar).
3. Escolha OK.

Parte 6: Atualizar as configurações de gerenciamento de energia

A seguinte atualização das configurações de gerenciamento de energia definirá os vídeos para nunca desligarem, o que permite desligamentos normais do sistema operacional no sistema Nitro. Todas as AMIs do Windows fornecidas pela Amazon a partir de 2018.11.28 já têm essa configuração padrão.

1. Abra um prompt de comando ou uma sessão do PowerShell.
2. Execute os seguintes comandos:

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Parte 7: Atualizar drivers do chipset Intel para novos tipos de instância

Os tipos de instância `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` usam hardware que exige drivers de chipset que não foram instalados anteriormente nas AMIs do Windows. Se você não estiver usando uma instância executada de uma AMI do Windows fornecida pela Amazon, datada de 19/11/2018 ou posterior, deverá instalar os drivers usando o utilitário INF do Chipset Intel.

Para instalar os drivers de chipset

1. [Faça download do utilitário chipset](#) na instância.
2. Extraia os arquivos.
3. Executar `SetupChipset.exe`.
4. Aceite o contrato de licença do software Intel e instale os drivers do chipset.
5. Reinicialize a instância.

(Alternativa) Atualizar os drivers PV, ENA e NVMe da AWS usando o AWS Systems Manager

O documento de automação do AWSSupport-UpgradeWindowsAWSDrivers automatiza as etapas descritas em Parte 1, Parte 2 e Parte 3. Esse método também pode reparar uma instância onde houve falha nas atualizações de driver.

O documento de automação do AWSSupport-UpgradeWindowsAWSDrivers atualiza ou repara os drivers AWS de armazenamento e rede na instância do EC2 especificada. O documento tenta instalar as versões mais recentes dos drivers da AWS online chamando o AWS Systems Manager Agent (SSM Agent). Se o SSM Agent não puder ser conectado, o documento poderá executar uma instalação offline dos drivers da AWS caso solicitado explicitamente.

Note

Esse procedimento falhará em um controlador de domínio. Para atualizar drivers em um controlador de domínio, consulte [Atualizar um controlador de domínio \(atualização do AWS PV\) \(p. 567\)](#).

Como atualizar automaticamente os drivers AWS PV, ENA e NVMe usando AWS Systems Manager

1. Abra o console do Systems Manager em <https://console.aws.amazon.com/systems-manager>.
2. Escolha Automation (Automação), Execute Automation (Executar automação).
3. Escolha o documento de automação AWSSupport-UpgradeWindowsAWSDrivers e configure as seguintes opções na seção Parâmetros de entrada:

ID da instância

Insira o ID exclusivo da instância a ser atualizada.

AllowOffline

(Opcional) Escolha uma das seguintes opções:

- **True:** escolha essa opção para executar uma instalação offline. A instância é interrompida e reiniciada durante o processo de atualização.

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para preservar dados em volumes de armazenamento de instâncias, faça backup dos dados no armazenamento persistente.

- **False:** (Padrão) para executar uma instalação online, deixe essa opção selecionada. A instância é reiniciada durante o processo de atualização.

Important

As atualizações online e offline criam uma AMI antes de tentar as operações de atualização. A AMI persiste depois da conclusão da automação. Garanta seu acesso à AMI ou exclua-o se não for necessário.

SubnetId

(Opcional) Insira um dos seguintes valores:

- **SelectedInstanceSubnet** — (Padrão) O processo de atualização executa a instância helper na mesma sub-rede da instância que deve ser atualizada. A sub-rede deve permitir a comunicação com os endpoints Systems Manager (`ssm.*`).
- **CreateNewVPC** — O processo de atualização executa a instância helper em uma nova VPC. Use essa opção se não souber ao certo se a sub-rede da instância de destino permite a

comunicação com os endpoints `ssm.*`. O usuário do IAM deve ter permissão para criar uma VPC.

- Um ID de sub-rede específico — Especifique o ID de uma sub-rede específica na qual executar a instância helper. A sub-rede na mesma zona de disponibilidade da instância que deve ser atualizada, e deve permitir a comunicação com os endpoints `ssm.*`.
4. Escolha Execute automation.
 5. Deixe a atualização terminar. Pode levar até 10 minutos para concluir uma atualização online e até 25 minutos para concluir uma atualização offline.

Migrar para tipos de instância Xen a partir de tipos de instância Nitro

O procedimento a seguir pressupõe que você está executando em um tipo de instância baseada em Nitro, como M5 ou C5, e que você está migrando para uma instância baseada no Sistema Xen, como M4 ou C4. Para obter especificações sobre tipo de instância, consulte [Tipos de instância do Amazon EC2](#). Execute as seguintes etapas antes da migração para evitar erros durante o processo de inicialização.

1. AWSOs drivers PV devem ser instalados e atualizados em uma instância Nitro antes de migrar para uma instância Xen. Para as etapas de instalação e atualização de drivers AWS PV, consulte [Parte 1: Instalar e atualizar drivers da AWS PV \(p. 689\)](#).
2. Atualize para a versão EC2Launch v2 mais recente. Consulte as etapas em [Migrar para o EC2Launch v2 \(p. 488\)](#).
3. Abra uma sessão do PowerShell e execute o seguinte comando como administrador para fazer o sysprep dos drivers do dispositivo. A execução do sysprep garante que os drivers de armazenamento de inicialização antecipada necessários para inicializar em instâncias Xen sejam devidamente registrados no Windows.

Note

Executar o comando usando as versões do PowerShell (x86) resultará em um erro. Este comando adiciona apenas os drivers de dispositivo críticos de inicialização ao banco de dados crítico do dispositivo. Não executa uma preparação de sysprep completa.

```
Start-Process rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
```

4. Execute a migração para um tipo de instância Xen quando o processo de sysprep for concluído.

Assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server

O serviço de assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server é uma ferramenta de script. Ele ajuda a mover workloads existentes do Microsoft SQL Server de um sistema operacional Windows para um Linux. Você pode usar o assistente de mudança de plataforma com qualquer máquina virtual (VM) do Windows Server hospedada na nuvem ou com ambientes locais que executam o Microsoft SQL Server 2008 e posterior. A ferramenta verifica as incompatibilidades comuns, exporta bancos de dados da VM do Windows e os importa para uma instância do EC2 executando o Microsoft SQL Server 2017 no Ubuntu 16.04. O processo automatizado resulta em uma VM do Linux pronta para ser utilizada, configurada com os bancos de dados do SQL Server que podem ser usados para experimentação e teste.

Tópicos

- [Concepts \(p. 695\)](#)
- [Serviços relacionados \(p. 695\)](#)
- [Como funciona o assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server \(p. 695\)](#)
- [Components \(p. 696\)](#)
- [Configuração \(p. 696\)](#)
- [Conceitos básicos \(p. 698\)](#)

Concepts

A terminologia e os conceitos a seguir são essenciais para que você entenda e use o assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server.

Backup

Um backup do Microsoft SQL Server copia os dados ou registra logs de um banco de dados do Microsoft SQL Server ou transações para um dispositivo de backup, como um disco. Para obter mais informações, consulte [Visão geral do backup \(Microsoft SQL Server\)](#).

Restaurar

Uma sequência lógica e significativa para recuperar um conjunto de backups do Microsoft SQL Server. Para obter mais informações, consulte [Visão geral da restauração e recuperação \(Microsoft SQL Server\)](#).

Realocação de plataformas

Um banco de dados do Microsoft SQL Server pode ser realocado de uma instância do EC2 do Windows para uma instância do EC2 do Linux que esteja executando o Microsoft SQL Server. Ele também pode ser realocado para o VMware Cloud que executa o Microsoft SQL Server Linux na AWS.

Serviços relacionados

O [AWS Systems Manager \(Systems Manager\)](#) oferece visibilidade e controle da infraestrutura na AWS. O assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server usa o Systems Manager para mover seus bancos de dados do Microsoft SQL para o Microsoft SQL Server no EC2 do Linux. Para obter mais informações sobre o Systems Manager, consulte o [AWS Systems Manager User Guide \(Manual do usuário do AWS Systems Manager\)](#).

Como funciona o assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server

O assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server permite migrar seus bancos de dados do Microsoft SQL Server de um ambiente local ou uma instância EC2 do Windows para o Microsoft SQL Server 2017 no EC2 do Linux usando backup e restauração. Para a instância do EC2 do Linux de destino, forneça o ID ou o tipo de instância com o ID da sub-rede e o par de chaves do EC2.

Quando você executa o script PowerShell para o assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server nos bancos de dados de origem do Microsoft SQL Server, a instância do Windows faz um backup dos bancos de dados para um bucket de armazenamento criptografado do [Amazon Simple Storage Service \(S3\)](#). Então, ele recupera o backup para um Microsoft SQL Server existente na instância do EC2 do Linux, ou inicia um novo Microsoft SQL Server na instância do EC2 do Linux e faz backup para a instância recém-criada. Esse processo pode ser usado para

a realocação de plataformas dos seus bancos de dados de dois níveis que executam aplicações empresariais. Ele também permite replicar seu banco de dados para o Microsoft SQL Server no Linux para testar a aplicação enquanto o Microsoft SQL Server de origem permanece online. Após o teste, você pode agendar um tempo de inatividade da aplicação e executar novamente o script de backup PowerShell durante a migração final.

O processo inteiro de realocação de plataformas também pode ser automatizado e executado sem supervisão. Você pode executar o documento do SSM do Systems Manager [AWSEC2-SQLServerDBRestore](#) para importar os arquivos existentes de backup de banco de dados para o Microsoft SQL Server no EC2 do Linux sem usar o script de backup PowerShell.

Components

O script do assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server tem dois componentes principais:

1. Um [script de backup PowerShell](#), que faz backup no local dos bancos de dados do Microsoft SQL Server em um bucket de armazenamento do Amazon S3. Ele, então, invoca um documento de automação do SSM [AWSEC2-SQLServerDBRestore](#) para recuperar os backups para um Microsoft SQL Server na instância do EC2 do Linux.
2. Um documento de automação do SSM nomeado [AWSEC2-SQLServerDBRestore](#), que restaura os backups do banco de dados para o Microsoft SQL Server no EC2 do Linux. A automação restaura os backups de banco de dados do Microsoft SQL Server armazenados no Amazon S3 para o Microsoft SQL Server 2017 em execução em uma instância do EC2 do Linux. Você pode fornecer sua própria instância do EC2 que executa o Microsoft SQL Server 2017 Linux, ou a automação iniciará e configurará uma nova instância do EC2 com o Microsoft SQL Server 2017 no Ubuntu 16.04. A automação suporta a recuperação de backups de logs completos, diferenciais e transacionais, e aceita vários arquivos de backup de bancos de dados. A automação recupera automaticamente os backups válidos mais recentes de cada banco de dados nos arquivos fornecidos. Para mais informações, consulte [AWSEC2-SQLServerDBRestore](#).

Configuração

Esta seção cobre os passos necessários para executar o script de realocação de plataformas Windows para Linux.

Tópicos

- [Prerequisites \(p. 696\)](#)
- [Pré-requisitos para a realocação de plataformas para uma instância do EC2 existente \(p. 697\)](#)

Prerequisites

Para executar o script do assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server, você precisa fazer o seguinte:

1. Instalar o módulo PowerShell da AWS

Para instalar o módulo PowerShell da AWS, siga as etapas listadas em [Configurar o AWS Tools for PowerShell em um computador baseado em Windows](#). Recomendamos usar o PowerShell 3.0 ou mais recente para que o script de backup funcione corretamente.

2. Instalar o script de backup do PowerShell para o assistente de realocação de plataformas Windows para Linux.

Para executar o assistente de recolocação na plataforma do Windows para Linux, faça download do script de backup do PowerShell: [MigrateSQLServerToEC2Linux.ps1](#).

3. Adicionar um perfil de usuário da AWS ao armazenamento do AWS SDK

Para adicionar e configurar o perfil de usuário da AWS, veja as etapas listadas em [Gerenciar perfis](#) no Guia do usuário do AWS Tools for PowerShell. [Configure a seguinte política do IAM](#) para seu perfil de usuário. Você também pode adicionar essas permissões como uma política em linha sob a conta do usuário da AWS que usa o console do IAM.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RebootInstances",  
                "ec2:DescribeInstanceStatus",  
                "ec2:DescribeInstances",  
                "ec2>CreateTags",  
                "ec2:RunInstances",  
                "ec2:DescribeImages",  
                "iam:PassRole",  
                "ssm:StartAutomationExecution",  
                "ssm:DescribeInstanceInformation",  
                "ssm>ListCommandInvocations",  
                "ssm>ListCommands",  
                "ssm:SendCommand",  
                "ssm:GetAutomationExecution",  
                "ssm:GetCommandInvocation",  
                "s3:PutEncryptionConfiguration",  
                "s3>CreateBucket",  
                "s3>ListBucket",  
                "s3:PutObject",  
                "s3:GetObject",  
                "s3>DeleteObject",  
                "s3>DeleteBucket"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

4. Criar uma função do IAM de perfil de instância

Para criar um perfil de instância do IAM que execute o Systems Manager no EC2 do Linux, seve as etapas em [Create an Instance Profile for Systems Manager \(Criar um perfil de instância para o Systems Manager\)](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

Pré-requisitos para a realocação de plataformas para uma instância do EC2 existente

Para a realocação de plataformas para uma instância existente em execução no Microsoft SQL Server 2017 no Linux, você precisa:

1. Configurar um perfil de instância do EC2 com um perfil do AWS Identity and Access Management (IAM) e anexar a política gerenciada `AmazonSSMManagedInstanceCore`.

Para obter informações sobre como criar um perfil de instância do IAM para sua instância do Systems Manager, consulte os seguintes tópicos no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager):

- [Criar um perfil de instância para Systems Manager](#)

- [Anexar um perfil de instância do IAM a uma instância do Amazon EC2](#)
2. Verifique se o SSM Agent está instalado na sua instância do EC2. Para obter mais informações, consulte [Installing and Configuring SSM Agent on Windows Instances \(Instalar e configurar o SSM Agent em instâncias do Windows\)](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).
 3. Verifique se a instância do EC2 tem espaço em disco suficiente para fazer o download e a restauração dos backups do Microsoft SQL Server.

Conceitos básicos

Esta seção contém as definições do parâmetro PowerShell e os scripts para a realocação de plataformas dos seus bancos de dados. Para mais informações sobre como utilizar os scripts PowerShell, consulte [PowerShell](#).

Tópicos

- [Executar o assistente de realocação de plataformas Windows para Linux para script do Microsoft SQL Server \(p. 698\)](#)
- [Parameters \(p. 699\)](#)

Executar o assistente de realocação de plataformas Windows para Linux para script do Microsoft SQL Server

Os cenários comuns e exemplos de scripts PowerShell a seguir mostram como fazer a realocação de plataformas dos seus bancos de dados do Microsoft SQL Server usando o assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server.

Important

O assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server redefine a senha do usuário administrador (SA) do servidor do SQL Server na instância de destino toda vez que ele é executado. Depois que a realocação termina, é necessário definir sua própria senha para o usuário SA antes de conectar à instância de destino do SQL Server.

Syntax

O script do assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server adere à sintaxe exibida no exemplo a seguir.

```
PS C:\> C:\MigrateSQLServerToEC2Linux.ps1 [[-SqlServerInstanceName] <String>] [[-DBNames]<Object[]>] [-MigrateAllDBs] [PathForBackup] <String> [-SetSourceDBModeReadOnly] [-IamInstanceProfileName] <String>[-AWSRegion] <String> [[-EC2InstanceId] <String>] [[-EC2InstanceType] <String>] [[-EC2KeyPair] <String>] [[-SubnetId] <String>] [[-AWSProfileName] <String>] [[-AWSProfileLocation] <String>] [-GeneratePresignedUrls] [<CommonParameters>]
```

Exemplo 1: mover um banco de dados para uma instância do EC2

O exemplo a seguir mostra como mover um banco de dados chamado AdventureDB para uma instância do EC2 do Linux no Microsoft SQL Server, com o ID da instância sendo i-024689abcdef, de uma instância do Microsoft SQL Server chamada MSSQLSERVER. O diretório de backup a ser usado é D:\Backup e a região da AWS é us-east-2.

```
PS C:\> ./MigrateSQLServerToEC2Linux.ps1 - SQLServerInstanceName MSSQLSERVER -  
EC2InstanceId i-024689abcdef -DBNames AdventureDB -PathForBackup D:\\\\Backup -AWSRegion us-east-2 -  
IamInstanceProfileName AmazonSSMManagedInstanceCore
```

Exemplo 2: mover um banco de dados para uma instância do EC2 usando o perfil de credenciais da AWS

O exemplo a seguir mostra como mover o banco de dados do exemplo 1 usando o perfil de credenciais da AWS: **DBMigration**.

```
PS C:\> ./MigrateSQLServerToEC2Linux.ps1 - SQLServerInstanceName MSSQLSERVER -  
EC2InstanceId i-024689abcdef -DBNames AdventureDB -PathForBackup D:\\\\Backup -AWSRegion us-east-2 -  
AWSProfileName DBMigration -IamInstanceProfileName AmazonSSMManagedInstanceCore
```

Exemplo 3: mover um banco de dados para uma nova instância do tipo m5.large

O exemplo a seguir mostra como criar uma instância do EC2 do Linux do tipo m5.large na subnet-abc127 usando o par de chaves **customer-ec2-keypair** e movendo AdventureDB e TestDB para a nova instância do banco de dados usado nos exemplos 1 e 2.

```
PS C:\> ./MigrateSQLServerToEC2Linux.ps1 -EC2InstanceType m5.large -SubnetId subnet-abc127  
-EC2KeyPair customer-ec2-keypair -DBNames AdventureDB,TestDB -PathForBackup D:\\\\Backup -AWSRegion us-east-2 -  
AWSProfileName DBMigration -IamInstanceProfileName AmazonSSMManagedInstanceCore
```

Exemplo 4: mover todos os bancos de dados para uma nova instância do tipo m5.large

O exemplo a seguir mostra como criar uma instância do EC2 do Linux do tipo m5.large na subnet-abc127 usando o par de chaves **customer-ec2-keypair** e migrando todos os bancos de dados para a instância dos bancos de dados usados nos exemplos 1 e 2.

```
PS C:\> ./MigrateSQLServerToEC2Linux.ps1 -EC2InstanceType m5.large -SubnetId subnet-abc127  
-EC2KeyPair customer-ec2-keypair -MigrateAllDBs -PathForBackup D:\\\\Backup -AWSRegion us-east-2 -  
AWSProfileName DBMigration -IamInstanceProfileName AmazonSSMManagedInstanceCore
```

Parameters

Os parâmetros a seguir são utilizados pelo script PowerShell para realocar seus bancos de dados do Microsoft SQL Server.

-SqlServerInstanceName

O nome da instância do Microsoft SQL Server para backup. Se o valor de **SqlServerInstanceName** não for fornecido, **\$env:ComputerName** será usado por padrão.

Tipo: string

Exigido: Não

-DBNames

Os nomes dos bancos de dados para backup e recuperação. Especifique os nomes dos bancos de dados em uma lista separada por vírgulas (por exemplo, **adventureDB,universityDB**). Um dos parâmetros, **DBNames** ou **MigrateAllDBs**, é obrigatório.

Tipo: objeto

Exigido: Não

-MigrateAllDBs

O switch é desabilitado por padrão. Se o switch estiver ativado, a automação migrará todos os bancos de dados exceto os bancos de dados do sistema (master, msdb, tempdb). Um dos parâmetros, DBNames ou MigrateAllDBs, é obrigatório.

Tipo: SwitchParameter

Exigido: Não

-PathForBackup

O caminho para o local em que o backup completo está salvo.

Tipo: string

Obrigatório: sim

-SetSourceDBModeReadOnly

O switch é desabilitado por padrão. Se o switch estiver habilitado, ele fará o banco de dados ser somente de leitura durante a migração.

Tipo: SwitchParameter

Exigido: Não

-IamInstanceProfileName

Insira a função da instância do AWS IAM com as permissões para executar a automação do Systems Manager em seu nome. Consulte [Getting Started with Automation \(Conceitos básicos da automação\)](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager).

Tipo: string

Obrigatório: sim

-AWSRegion

Insira a região da AWS onde os buckets do Amazon S3 foram criados para guardar os backups dos bancos de dados.

Tipo: string

Obrigatório: sim

-EC2InstanceId

Para restaurar os bancos de dados do Microsoft SQL Server para uma instância do EC2 existente executando o Microsoft SQL Server Linux, insira o ID da instância. Verifique se a instância do EC2 já tem o [SSM Agent do AWS Systems Manager instalado e em funcionamento](#).

Tipo: string

Exigido: Não

-EC2InstanceType

Para restaurar os bancos de dados do Microsoft SQL Server para uma nova instância do EC2 do Linux, insira o tipo da instância que será iniciada.

Tipo: string

Exigido: Não

-EC2KeyPair

Para restaurar os bancos de dados do Microsoft SQL Server para a nova instância EC2 do Linux, insira o nome do par de chaves do EC2 que será usado para acessar a instância. Esse parâmetro é necessário se você estiver criando uma nova instância do EC2 do Linux.

Tipo: string

Exigido: Não

-SubnetId

Esse parâmetro é necessário para criar uma nova instância do EC2 do Linux. Ao criar uma nova instância do EC2 do Linux, se o SubnetId não for fornecido, a sub-rede padrão do usuário da AWS será utilizada para iniciar a instância do EC2 do Linux.

Tipo: string

Exigido: Não

-AWSProfileName

O nome do perfil da AWS que a automação usa quando conecta aos serviços da AWS. Para obter mais informações sobre as permissões necessárias do usuário do IAM, consulte [Getting Started with Automation \(Conceitos básicos da automação\)](#) no AWS Systems Manager User Guide (Manual do usuário do AWS Systems Manager). Se um perfil não for inserido, a automação usará o perfil padrão da AWS.

Tipo: string

Exigido: Não

-AWSProfileLocation

A localização do perfil da AWS se o perfil AWS não estiver armazenado no local padrão.

Tipo: string

Exigido: Não

-GeneratePresignedUrls

Esse parâmetro é usado apenas para a realocação de plataformas de instâncias não EC2, como VMware Cloud na AWS ou VMs no local.

Tipo: SwitchParameter

Exigido: Não

<CommonParameters>

Esse cmdlet é compatível com os parâmetros comuns: `Verbose`, `Debug`, `ErrorAction`, `ErrorVariable`, `WarningAction`, `WarningVariable`, `OutBuffer`, `PipelineVariable` e `OutVariable`. Para mais informações, consulte [Sobre os parâmetros comuns](#) na documentação do Microsoft PowerShell.

Exigido: Não

Solucionar problemas de uma atualização

A AWS oferece suporte à atualização para problemas com o Upgrade Helper Service, um utilitário da AWS que ajuda você a executar atualizações no local que envolvem drivers Citrix PV.

Após a atualização, a instância pode apresentar temporariamente uma utilização de CPU maior do que a média enquanto o serviço .NET Runtime Optimization otimiza o .NET Framework. Esse comportamento é esperado.

Se a instância não passou nas duas verificações de status após várias horas, verifique o seguinte.

- Se você fez a atualização para o Windows Server 2008 e as duas verificações de status falharem após várias horas, a atualização pode ter falhado e estar apresentando um prompt para Clicar em OK a fim de confirmar a reversão. Como o console não está acessível nesse estado, não há como clicar no botão. Para contornar isso, execute uma reinicialização através da API ou do console do Amazon EC2. A reinicialização levará 10 minutos ou mais para ser iniciada. A instância pode se tornar disponível após 25 minutos.
- Remova as aplicações ou as funções do servidor e tente novamente.

Se a instância não passar nas verificações de status depois de remover as aplicações ou funções do servidor, faça o seguinte.

- Interrompa a instância e anexe o volume raiz a outra instância. Para obter mais informações, consulte a descrição de como parar e anexar o volume raiz a outra instância em "[Esperando o serviço de metadados](#)" (p. 1640).
- Analise os arquivos de log de configuração do Windows e os logs de eventos para ver se há falhas.

Para outros problemas com uma atualização ou uma migração do sistema operacional, recomendamos analisar os artigos indicados em [Antes de iniciar uma atualização no local](#) (p. 677).

Identificar as instâncias do Windows do EC2

Sua aplicação pode precisar determinar se está executando em uma instância do EC2.

Para obter informações sobre como identificar as instâncias Linux, consulte [Identify EC2 Linux instances](#) (Identificar instâncias Linux do EC2) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Inspecione o documento de identidade da instância

Para um método definitivo e criptograficamente verificado de identificação de uma instância do EC2, verifique o documento de identidade da instância, incluindo sua assinatura. Esses documentos estão disponíveis em cada instância do EC2 no endereço local não roteável `http://169.254.169.254/latest/dynamic/instance-identity/`. Para obter mais informações, consulte [Documentos de identidade da instância](#) (p. 648).

Inspecione o UUID do sistema

Você pode obter o UUID do sistema e procurar pela presença dos caracteres ou "EC2" no octeto inicial do UUID. O método para determinar se um sistema é uma instância do EC2 é rápido, mas potencialmente

impreciso, pois há uma pequena possibilidade de um sistema que não seja uma instância do EC2 ter um UUID que comece com esses caracteres. Além disso, as instâncias do EC2 que usam o SMBIOS 2.4 podem representar o UUID em formato little-endian e, portanto, os caracteres "EC2" não aparecem no início do UUID.

Example : Obter o UUID usando o WMI ou o Windows PowerShell

Use a linha de comando de Instrumentação de Gerenciamento do Windows (WMIC) da seguinte forma:

```
wmic path win32_computersystemproduct get uuid
```

Alternativamente, se você estiver usando o Windows PowerShell, use o cmdlet Get-WmiObject da seguinte maneira:

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select UUID
```

Na próxima saída de exemplo, o UUID começa com "EC2", que indica que o sistema é provavelmente uma instância do EC2.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Para instâncias que usam o SMBIOS 2.4, o UUID pode ser representado no formato little-endian; por exemplo:

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Tutorial: Configurar um cluster do Windows HPC no Amazon EC2

Você pode executar um cluster escalável do Windows High Performance Computing (HPC) usando instâncias do Amazon EC2. Um cluster do Windows HPC exige um controlador de domínio do Active Directory, um servidor DNS, um nó de cabeçalho e um ou mais nós de computação.

Para configurar um cluster do Windows HPC no Amazon EC2, execute as seguintes tarefas:

- [Etapa 1: Criar seus grupos de segurança \(p. 704\)](#)
- [Etapa 2: Configurar o controlador de domínio do Active Directory \(p. 706\)](#)
- [Etapa 3: Configurar o nó do cabeçalho \(p. 707\)](#)
- [Etapa 4: Configurar o nó de computação \(p. 709\)](#)
- [Etapa 5: Dimensione seus nós de computação de HPC \(opcional\) \(p. 710\)](#)

Para obter mais informações sobre computação de alta performance, consulte [High Performance Computing \(HPC\) na AWS \(Computação de Alta Performance \(HPC\) na AWS\)](#).

Prerequisites

Você deve executar suas instâncias em uma VPC. Você pode usar a VPC padrão ou criar uma VPC não padrão. Para obter mais informações, consulte [Conceitos básicos](#) no Guia do usuário da Amazon VPC.

Etapa 1: Criar seus grupos de segurança

Use o Tools for Windows PowerShell para criar security groups para o controlador do domínio, membros do domínio e cluster de HPC.

Para criar os security groups

1. Use o cmdlet [New-EC2SecurityGroup](#) para criar o grupo de segurança do controlador de domínio. Observe o ID do security group na saída.

```
PS C:\> New-EC2SecurityGroup -VpcId vpc-id -GroupName "SG - Domain Controller" -Description "Active Directory Domain Controller"
```

2. Use o cmdlet [New-EC2SecurityGroup](#) para criar o grupo de segurança para os membros do domínio. Observe o ID do security group na saída.

```
PS C:\> New-EC2SecurityGroup -VpcId vpc-id -GroupName "SG - Domain Member" -Description "Active Directory Domain Member"
```

3. Use o cmdlet [New-EC2SecurityGroup](#) para criar o grupo de segurança para o cluster de HPC. Observe o ID do security group na saída.

```
PS C:\> New-EC2SecurityGroup -VpcId vpc-id -GroupName "SG - Windows HPC Cluster" -Description "Windows HPC Cluster Nodes"
```

Para adicionar regras aos security groups

1. Crie as regras a seguir para adicionar ao security group do controlador de domínio. Substitua o ID do security group de placeholder pelo ID do security group do membro do domínio e o bloco CIDR do placeholder pelo bloco CIDR da sua rede.

```
PS C:\> $sg_dm = New-Object Amazon.EC2.Model.UserIdGroupPair
PS C:\> $sg_dm.GroupId = "sg-12345678
PS C:\> $r1 = @{ IpProtocol="UDP"; FromPort="123"; ToPort="123"; UserIdGroupPairs=$sg_dm }
PS C:\> $r2 = @{ IpProtocol="TCP"; FromPort="135"; ToPort="135"; UserIdGroupPairs=$sg_dm }
PS C:\> $r3 = @{ IpProtocol="UDP"; FromPort="138"; ToPort="138"; UserIdGroupPairs=$sg_dm }
PS C:\> $r4 = @{ IpProtocol="TCP"; FromPort="49152"; ToPort="65535"; UserIdGroupPairs=$sg_dm }
PS C:\> $r5 = @{ IpProtocol="TCP"; FromPort="389"; ToPort="389"; UserIdGroupPairs=$sg_dm }
PS C:\> $r6 = @{ IpProtocol="UDP"; FromPort="389"; ToPort="389"; UserIdGroupPairs=$sg_dm }
PS C:\> $r7 = @{ IpProtocol="TCP"; FromPort="636"; ToPort="636"; UserIdGroupPairs=$sg_dm }
PS C:\> $r8 = @{ IpProtocol="TCP"; FromPort="3268"; ToPort="3269"; UserIdGroupPairs=$sg_dm }
PS C:\> $r9 = @{ IpProtocol="TCP"; FromPort="53"; ToPort="53"; UserIdGroupPairs=$sg_dm }
PS C:\> $r10 = @{ IpProtocol="UDP"; FromPort="53"; ToPort="53"; UserIdGroupPairs=$sg_dm }
PS C:\> $r11 = @{ IpProtocol="TCP"; FromPort="88"; ToPort="88"; UserIdGroupPairs=$sg_dm }
PS C:\> $r12 = @{ IpProtocol="UDP"; FromPort="88"; ToPort="88"; UserIdGroupPairs=$sg_dm }
PS C:\> $r13 = @{ IpProtocol="TCP"; FromPort="445"; ToPort="445"; UserIdGroupPairs=$sg_dm }
```

```
PS C:\> $r14 = @{ IpProtocol="UDP"; FromPort="445"; ToPort="445"; UserIdGroupPairs=$sg_dm }
PS C:\> $r15 = @{ IpProtocol="ICMP"; FromPort="-1"; ToPort="-1"; UserIdGroupPairs=$sg_dm }
PS C:\> $r16 = @{ IpProtocol="UDP"; FromPort="53"; ToPort="53";
IpRanges="203.0.113.25/32" }
PS C:\> $r17 = @{ IpProtocol="TCP"; FromPort="3389"; ToPort="3389";
IpRanges="203.0.113.25/32" }
```

2. Use o cmdlet [Grant-EC2SecurityGroupIngress](#) para adicionar as regras ao grupo de segurança do controlador de domínio.

```
PS C:\> Grant-EC2SecurityGroupIngress -GroupId sg-1a2b3c4d -IpPermission @($r1, $r2,
$r3, $r4, $r5, $r6, $r7, $r8, $r9, $r10, $r11, $r12, $r13, $r14, $r15, $r16, $r17)
```

Para obter mais informações sobre essas regras do security group, consulte o seguinte artigo da Microsoft: [Como configurar um firewall para domínios e relações de confiança](#).

3. Crie as regras a seguir para adicionar o security group do membro do domínio. Substitua o ID do security group do placeholder pelo ID do security group do controlador do domínio.

```
PS C:\> $sg_dc = New-Object Amazon.EC2.Model.UserIdGroupPair
PS C:\> $sg_dc.GroupId = "sg-1a2b3c4d
PS C:\> $r1 = @{ IpProtocol="TCP"; FromPort="49152"; ToPort="65535"; UserIdGroupPairs=$sg_dc }
PS C:\> $r2 = @{ IpProtocol="UDP"; FromPort="49152"; ToPort="65535"; UserIdGroupPairs=$sg_dc }
PS C:\> $r3 = @{ IpProtocol="TCP"; FromPort="53"; ToPort="53"; UserIdGroupPairs=$sg_dc }
PS C:\> $r4 = @{ IpProtocol="UDP"; FromPort="53"; ToPort="53"; UserIdGroupPairs=$sg_dc }
```

4. Use o cmdlet [Grant-EC2SecurityGroupIngress](#) para adicionar as regras ao grupo de segurança do membro do domínio.

```
PS C:\> Grant-EC2SecurityGroupIngress -GroupId sg-12345678 -IpPermission @($r1, $r2,
$r3, $r4)
```

5. Crie as regras a seguir para adicionar o security group do cluster de HPC. Substitua ID do security group do placeholder pelo ID do security group do cluster de HPC e o bloco CIDR do placeholder pelo bloco CIDR da sua rede.

```
$sg_hpc = New-Object Amazon.EC2.Model.UserIdGroupPair
PS C:\> $sg_hpc.GroupId = "sg-87654321
PS C:\> $r1 = @{ IpProtocol="TCP"; FromPort="80"; ToPort="80"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r2 = @{ IpProtocol="TCP"; FromPort="443"; ToPort="443"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r3 = @{ IpProtocol="TCP"; FromPort="1856"; ToPort="1856"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r4 = @{ IpProtocol="TCP"; FromPort="5800"; ToPort="5800"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r5 = @{ IpProtocol="TCP"; FromPort="5801"; ToPort="5801"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r6 = @{ IpProtocol="TCP"; FromPort="5969"; ToPort="5969"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r7 = @{ IpProtocol="TCP"; FromPort="5970"; ToPort="5970"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r8 = @{ IpProtocol="TCP"; FromPort="5974"; ToPort="5974"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r9 = @{ IpProtocol="TCP"; FromPort="5999"; ToPort="5999"; UserIdGroupPairs=$sg_hpc }
```

```
PS C:\> $r10 = @{ IpProtocol="TCP"; FromPort="6729"; ToPort="6730"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r11 = @{ IpProtocol="TCP"; FromPort="7997"; ToPort="7997"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r12 = @{ IpProtocol="TCP"; FromPort="8677"; ToPort="8677"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r13 = @{ IpProtocol="TCP"; FromPort="9087"; ToPort="9087"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r14 = @{ IpProtocol="TCP"; FromPort="9090"; ToPort="9092"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r15 = @{ IpProtocol="TCP"; FromPort="9100"; ToPort="9163"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r16 = @{ IpProtocol="TCP"; FromPort="9200"; ToPort="9263"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r17 = @{ IpProtocol="TCP"; FromPort="9794"; ToPort="9794"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r18 = @{ IpProtocol="TCP"; FromPort="9892"; ToPort="9893"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r19 = @{ IpProtocol="UDP"; FromPort="9893"; ToPort="9893"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r20 = @{ IpProtocol="TCP"; FromPort="6498"; ToPort="6498"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r21 = @{ IpProtocol="TCP"; FromPort="7998"; ToPort="7998"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r22 = @{ IpProtocol="TCP"; FromPort="8050"; ToPort="8050"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r23 = @{ IpProtocol="TCP"; FromPort="5051"; ToPort="5051"; UserIdGroupPairs=$sg_hpc }
PS C:\> $r24 = @{ IpProtocol="TCP"; FromPort="3389"; ToPort="3389"; IpRanges="203.0.113.25/32" }
```

6. Use o cmdlet [Grant-EC2SecurityGroupIngress](#) para adicionar as regras ao grupo de segurança do cluster de HPC.

```
PS C:\> Grant-EC2SecurityGroupIngress -GroupId sg-87654321 -IpPermission @($r1, $r2, $r3, $r4, $r5, $r6, $r7, $r8, $r9, $r10, $r11, $r12, $r13, $r14, $r15, $r16, $r17, $r18, $r19, $r20, $r21, $r22, $r23, $r24)
```

Para obter mais informações sobre essas regras do security group, consulte o seguinte artigo da Microsoft: [Redes do cluster de HPC: configuração do firewall Windows](#).

7. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
8. No painel de navegação, selecione Grupos de segurança. Verifique se todos os três security groups estão exibidos na lista e contêm as regras necessárias.

Etapa 2: Configurar o controlador de domínio do Active Directory

O controlador de domínio do Active Directory fornece autenticação e gerenciamento centralizado de recursos do ambiente HPC e é necessário para a instalação. Para configurar seu Active Directory, execute uma instância para servir como o controlador de domínio para seu cluster de HPC e configure-a.

Para executar um controlador de domínio para seu cluster de HPC

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel do console, escolha Executar instância.
3. Na página Escolher uma AMI, selecione uma AMI para o Windows Server e escolha Selecionar.

4. Na próxima página do assistente, selecione um tipo de instância e escolha Próximo: Configurar detalhes da instância.
5. Na página Configurar detalhes da instância, selecione sua VPC em Rede e uma sub-rede em Sub-rede. Na página seguinte do assistente, você pode especificar armazenamento adicional para sua instância.
6. Na página Adicionar tags, insira Domain Controller como valor para a tag Name da instância e escolha Próximo: Configurar security group.
7. Na página Configurar security group, escolha Selecionar um security group existente, escolha security group SG – Domain Controller e escolha então Revisar e executar.
8. Escolha Executar.
9. No painel de navegação, escolha Elastic IPs.
10. Escolha Allocate new address. Escolha Allocate. Escolha Close (Fechar).
11. Selecione o endereço IP elástico criado e escolha Ações, Associar endereço. Em Instância, escolha a instância do controlador de domínio. Escolha Associate.

Conecte-se à instância que você criou e configure o servidor como controlador de domínio para o cluster de HPC.

Para configurar sua instância como controlador de domínio

1. Conecte-se à sua instância Domain Controller. Para obter mais informações, acesse [Connect to your Windows Instance \(Conectar-se à sua instância do Windows\)](#).
2. Abra o Gerenciador de Servidores e adicione a função Serviços de Domínio do Active Directory.
3. Promova o servidor a um controlador de domínio usando o Gerenciador de Servidores ou executando DCPromo.exe.
4. Crie um novo domínio em uma nova floresta.
5. Digite **hpc.local** como nome de domínio totalmente qualificado (FQDN).
6. Selecione Nível funcional da floresta como Windows Server 2008 R2.
7. Certifique-se de que a opção Servidor DNS está selecionada e escolha Próximo.
8. Selecione Sim, o computador usará um endereço IP atribuído automaticamente por um servidor DHCP (não recomendado).
9. Quando solicitado, selecione Sim para continuar.
10. Conclua o assistente e selecione Reiniciar ao concluir.
11. Conecte-se à instância como **hpc.local\administrator**.
12. Crie um usuário de domínio **hpc.local\hpcuser**.

Etapa 3: Configurar o nó do cabeçalho

Um cliente HPC se conecta ao nó do cabeçalho. O nó do cabeçalho facilita os trabalhos programados. Você configura seu nó do cabeçalho executando uma instância, instalando o HPC Pack e configurando o cluster.

Execute uma instância e, em seguida, configure-a como membro do domínio **hpc.local** e com as contas de usuário necessárias.

Para configurar uma instância como seu nó principal

1. Execute uma instância e dê o nome de **HPC-Head**. Quando você executar a instância, selecione os dois security group: SG – cluster do Windows HPC e SG – membro do domínio.
2. Conecte-se à instância e obtenha o endereço do servidor DNS existente usando o seguinte comando:

```
IPConfig /all
```

3. Atualize as propriedades de TCP/IPv4 do NIC HPC-Head para incluir um endereço IP elástico para a instância Domain Controller como DNS primário e, em seguida, adicione o endereço IP do DNS adicional pela etapa anterior.
4. Adicione a máquina ao domínio hpc.local usando as credenciais para hpc.local\administrator (a conta de administrador de domínio).
5. Adicione hpc.local\hpcuser como administrador local. Quando as credenciais forem solicitadas, use hpc.local\administrator e reinicie a instância.
6. Conecte-se a HPC-Head como hpc.local\hpcuser.

Para instalar o HPC Pack

1. Conecte-se à sua instância HPC-Head usando a conta hpc.local\hpcuser.
2. Usando Gerenciador de Servidores, desative Configuração de segurança reforçada do Internet Explorer (ESC do IE) para Administradores.
 - a. Em Gerenciador de Servidores, sob Informações de Segurança, escolha Configurar ESC do IE.
 - b. Desative o ESC do IE para administradores.
3. Instale o HPC Pack em HPC-Head.
 - a. Faça download do HPC Pack para HPC-Head em [Central de Download da Microsoft](#). Escolha o HPC Pack para versão do Windows Server em HPC-Head.
 - b. Extraia arquivos para uma pasta, abra-a pasta e clique duas vezes sobre setup.exe.
 - c. Na página Instalação, selecione Criar novo cluster de HPC criando um nó de cabeçalho e selecione Próximo.
 - d. Aceite as configurações padrão para instalar todos os bancos de dados no nó de cabeçalho e selecione Próximo.
 - e. Assista todo o assistente.

Para configurar seu cluster de HPC no nós de cabeçalho

1. Inicie o HPC Cluster Manager.
2. Em Lista de tarefas de implantação, selecione Configurar sua rede.
 - a. No assistente, selecione a opção padrão (5) e escolha então Próximo.
 - b. Conclua o assistente aceitando os valores padrão em todas as telas e escolha como deseja atualizar o servidor e participar do feedback do cliente.
 - c. Selecione Configurar.
3. Selecione Fornecer credenciais de rede e insira as credenciais de hpc.local\hpcuser.
4. Selecione Configurar a nomeação de novos nós e escolha OK.
5. Selecione Criar um modelo de nó.
 - a. Selecione Calcular modelo de nó e escolha Próximo.
 - b. Selecione Sem sistema operacional e continue com os padrões.
 - c. Escolha Create (Criar).

Etapa 4: Configurar o nó de computação

Você configura o nó de computação executando uma instância, instalando o HPC Pack e adicionando o nó ao seu cluster.

Primeiro, execute uma instância e configure-a como membro do domínio `hpc.local` com as contas de usuário necessárias.

Para configurar uma instância para seu nó de computação

1. Execute uma instância e dê o nome de `HPC-Compute`. Quando você executar a instância, selecione os security group a seguir: SG – Cluster do Windows HPC e SG – Membro do domínio.
2. Faça login na instância e obtenha o endereço DNS existente do servidor em HPC-Compute usando o seguinte comando:

```
IPConfig /all
```

3. Atualize as propriedades de TCP/IPv4 do NIC `HPC-Compute` para incluir o endereço IP elástico da instância `Domain Controller` como DNS primário. Em seguida, adicione o endereço IP adicional do DNS da etapa anterior.
4. Adicione a máquina ao domínio `hpc.local` usando as credenciais para `hpc.local\administrator` (a conta de administrador de domínio).
5. Adicione `hpc.local\hpcuser` como administrador local. Quando as credenciais forem solicitadas, use `hpc.local\administrator` e reinicie.
6. Conecte-se a `HPC-Compute` como `hpc.local\hpcuser`.

Para instalar o HPC Pack no nó de computação

1. Conecte-se à sua instância `HPC-Compute` usando a conta `hpc.local\hpcuser`.
2. Usando Gerenciador de Servidores, desative Configuração de segurança reforçada do Internet Explorer (ESC do IE) para Administradores.
 - a. Em Gerenciador de Servidores, sob Informações de Segurança, escolha Configurar ESC do IE.
 - b. Desative o ESC do IE para administradores.
3. Instale o HPC Pack em `HPC-Compute`.
 - a. Faça download do HPC Pack para `HPC-Compute` em [Central de Download da Microsoft](#). Escolha o HPC Pack para versão do Windows Server em `HPC-Compute`.
 - b. Extraia arquivos para uma pasta, abra-a pasta e clique duas vezes sobre `setup.exe`.
 - c. Na página Instalação, selecione Juntar-se ao cluster HPC existente criando um novo nó de computação e escolha Próximo.
 - d. Especifique o nome totalmente qualificado da instância `HPC-Head` e escolha os padrões.
 - e. Assista todo o assistente.

Para concluir a configuração do seu cluster, vá ao nó principal e adicione o nó de computação ao seu cluster.

Para adicionar o nó de computação ao seu cluster

1. Conecte-se à instância `HPC-Head` como `hpc.local\hpcuser`.
2. Abra o HPC Cluster Manager.
3. Selecione Gerenciamento do nó.

-
4. Se o nó de computação for exibido no bucket Não aprovado, clique com o botão direito sobre o nó listado e selecione Adicionar nó.
 - a. Selecione Adicionar nós de computação ou nós de corretor que já tenham sido configurados.
 - b. Marque a caixa de seleção ao lado do nó e selecione Adicionar.
 5. Clique com o botão direito no nó e selecione Colocar online.

Etapa 5: Dimensione seus nós de computação de HPC (opcional)

Para dimensionar seus nós de computação

1. Conecte-se à instância HPC-Compute como hpc.local\hpcuser.
2. Exclua todos os arquivos que você baixou localmente do pacote de instalação do HP Pack. (Você já executou a configuração e criou esses arquivos na sua imagem, por isso eles não precisam ser clonados para uma AMI.)
3. Em C:\Program Files\Amazon\Ec2ConfigService, abra o arquivo sysprep2008.xml.
4. Na parte inferior de <settings pass="specialize">, adicione a seção a seguir. Substitua hpc.local, senha e hpcuser de acordo com seu ambiente.

```
<component name="Microsoft-Windows-UnattendedJoin" processorArchitecture="amd64"  
publicToken="31bf3856ad364e35"  
language="neutral" versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/  
WMIConfig/2002/State"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">  
    <Identification>  
        <UnsecureJoin>false</UnsecureJoin>  
        <Credentials>  
            <Domain>hpc.local</Domain>  
            <Password>password</Password>  
            <Username>hpcuser</Username>  
        </Credentials>  
        <JoinDomain>hpc.local</JoinDomain>  
    </Identification>  
</component>
```

5. Salvar sysprep2008.xml.
6. Escolha Iniciar, Todos os Programas, Configurações do EC2ConfigService.
 - a. Escolha a guia Geral e desmarque a caixa Definir nome do computador.
 - b. Escolha a guia Pacote e Executar Sysprep e desativar agora.
7. Abra o console do Amazon EC2.
8. No painel de navegação, escolha Instances (Instâncias).
9. Espere o status da instância mostrar Stopped (Interrompido).
10. Selecione a instância, escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).
11. Especifique um nome e uma descrição da imagem e escolha Create image (Criar imagem) para criar uma AMI da instância.
12. Execute a instância HPC-Compute original que foi fechada.
13. Conecte-se ao nó principal usando a conta hpc.local\hpcuser.
14. Pelo HPC Cluster Manager, exclua o nó antigo que agora aparece em estado de erro.
15. No console do Amazon EC2, no painel de navegação, selecione AMIs.

16. Use a AMI que você criou para adicionar nós adicionais ao cluster.

Você pode executar nós de computação adicionais pela AMI que criou. Esses nós são automaticamente juntados ao domínio, mas você deve adicioná-los ao cluster como nós já configurados em HPC Cluster Manager usando o nó de cabeçalho e colocando-o online.

Frota do EC2 e frota spot

Você pode usar uma EC2 Fleet ou uma frota spot para executar uma frota de instâncias. Em uma única chamada de API, uma frota pode executar vários tipos de instâncias em várias zonas de disponibilidade, usando as opções de compra Instância sob demanda, Instância reservada e Instância Spot juntas.

Tópicos

- [EC2 Fleet \(p. 712\)](#)
- [Frota spot \(p. 761\)](#)
- [Monitorar eventos da frota usando o Amazon EventBridge \(p. 799\)](#)
- [Tutoriais para EC2 Fleet e frota spot \(p. 813\)](#)
- [Exemplo de configurações para EC2 Fleet e frota spot \(p. 824\)](#)
- [Quotas da frota \(p. 848\)](#)

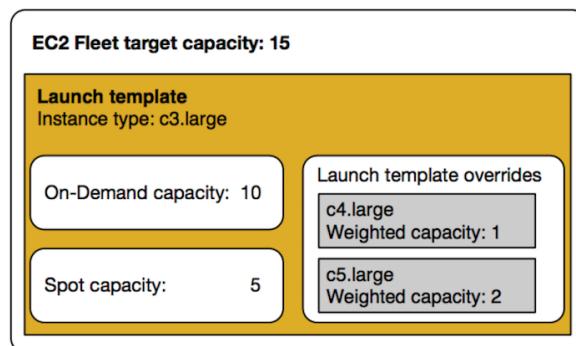
EC2 Fleet

Uma Frota do EC2 contém as informações de configuração para executar uma frota—ou um grupo—de instâncias. Em uma única chamada de API, uma frota pode executar vários tipos de instâncias em várias zonas de disponibilidade, usando as opções de compra Instância sob demanda, Instância reservada e Instância Spot juntas. Usando o Frota do EC2, você pode:

- Definir metas de capacidade sob demanda e Spot e a quantidade máxima que você está disposto a pagar por hora
- Especifique os tipos de instância que funcionam melhor para suas aplicações
- Especifique como o Amazon EC2 deve distribuir a capacidade da sua frota dentro de cada opção de compra

Você também poderá definir um valor máximo por hora que esteja disposto a pagar pela frota, e o Frota do EC2 executará instâncias até alcançar o valor máximo. Quando o valor máximo que você está disposto a pagar for alcançado, a frota interromperá a execução de instâncias mesmo que a capacidade de destino ainda não tenha sido alcançada.

A Frota do EC2 tenta executar o número de instâncias que são necessárias para atender à capacidade de destino especificada na sua solicitação. Se você tiver especificado um preço máximo total por hora, ele cumprirá a capacidade até alcançar a quantidade máxima que você está disposto a pagar. A frota também pode interromper a manutenção da capacidade Spot se as Instâncias spot forem interrompidas. Para obter mais informações, consulte [Como as Instâncias spot funcionam \(p. 304\)](#).



Você pode especificar um número ilimitado de tipos de instâncias por Frota do EC2. Esses tipos de instância podem ser provisionados usando as opções de compra sob demanda e spot. Você também pode especificar várias zonas de disponibilidade, especificar preços spot máximos diferentes para cada instância e escolher opções spot adicionais para cada frota. O Amazon EC2 usa as opções especificadas para provisionar capacidade quando a frota é iniciada.

Enquanto a frota estiver em execução, se o Amazon EC2 recuperar uma instância spot devido a um aumento de preço ou uma falha na instância, a EC2 Fleet tentará substituir as instâncias por qualquer um dos tipos de instância que você especificar. Isso facilita recuperar a capacidade durante um pico nos preços Spot. Você pode desenvolver uma estratégia flexível e elástica de alocação de recursos para cada frota. Por exemplo, dentro de frotas específicas, sua capacidade principal pode ser suplementada sob demanda com capacidade spot mais barata (se disponível).

Se você tiver Instâncias reservadas e especificar Instâncias on-demand na sua frota, a Frota do EC2 usará suas Instâncias reservadas. Por exemplo, se sua frota especificar instância sob demanda como `c4.large` e você tiver Instâncias reservadas para `c4.large`, receberá a definição de preço de Instância reservada.

Não há cobrança adicional pelo uso do Frota do EC2. Você paga apenas pelas instâncias do EC2 que a frota executar.

Tópicos

- [Limitações da Frota do EC2 \(p. 713\)](#)
- [Instâncias expansíveis \(p. 713\)](#)
- [Tipos de solicitação da Frota do EC2 \(p. 714\)](#)
- [Estratégias de configuração da Frota do EC2 \(p. 732\)](#)
- [Trabalhar com Frotas do EC2 \(p. 741\)](#)

Limitações da Frota do EC2

As limitações a seguir se aplicam à Frota do EC2:

- A EC2 Fleet está disponível apenas por meio da API ou da AWS CLI.
- Uma solicitação de EC2 Fleet não pode abranger regiões da AWS. Você precisa criar uma Frota do EC2 separada para cada região.
- Uma solicitação de Frota do EC2 não pode abranger sub-redes diferentes na mesma zona de disponibilidade.

Instâncias expansíveis

Se você executar as Instâncias spot usando um [tipo de instância expansível \(p. 169\)](#) e planeja usar as instâncias spot expansíveis imediatamente e por um breve período, sem tempo ocioso para acumular créditos de CPU, recomendamos executá-las no [modo padrão \(p. 185\)](#) para evitar pagar custos mais elevados. Se executar as Instâncias spot expansíveis no [modo ilimitado \(p. 177\)](#) e esgotar a CPU imediatamente, você gastará os créditos excedentes por isso. Se a instância for usada por um curto período, não haverá tempo para acumular créditos de CPU para pagamento dos créditos excedentes, e você precisará pagar os créditos excedentes ao encerrar a instância.

O modo ilimitado será adequado para instâncias spot expansíveis somente se a instância for executada por tempo suficiente para acumular créditos de CPU para intermitência. Caso contrário, pagar por créditos excedentes torna as instâncias spot expansíveis mais caras do que o uso de outras instâncias. Para obter mais informações, consulte [Quando usar o modo ilimitado versus CPU fixa \(p. 179\)](#).

Os créditos de lançamento são feitos para fornecer uma experiência de lançamento inicial produtiva para instâncias T2 fornecendo recursos computacionais suficientes para configurar a instância. Lançamentos

repetidos de instâncias T2 para acessar novos créditos de lançamento não são permitidos. Se você precisar de uma CPU sustentada, poderá obter créditos (ficando inativo durante um período), usar o [modo Ilimitado \(p. 177\)](#) para T2 Instâncias spot ou usar um tipo de instância com CPU dedicada.

Tipos de solicitação da Frota do EC2

Existem três tipos de solicitações de Frota do EC2:

`instant`

Se você configurar o tipo de solicitação como `instant`, a Frota do EC2 incluirá uma solicitação síncrona única da capacidade desejada. Na resposta da API, as instâncias que foram executadas são retornadas, junto com os erros das instâncias que não puderam ser executadas. Para obter mais informações, consulte [Usar uma EC2 Fleet do tipo 'instantâneo' \(p. 714\)](#).

`request`

Se você configurar o tipo de solicitação como `request`, a Frota do EC2 incluirá uma solicitação assíncrona única da capacidade desejada. Portanto, se a capacidade for reduzida devido a interrupções do spot, a frota não tentará reabastecer as Instâncias spot nem enviará solicitações em grupos de capacidade spot alternativos, se a capacidade não estiver disponível.

`maintain`

(Padrão) Se você configurar o tipo de solicitação como `maintain`, a Frota do EC2 incluirá uma solicitação assíncrona única da capacidade desejada e manterá a capacidade reabastecendo automaticamente quaisquer Instâncias spot interrompidas.

Todos os três tipos de solicitações se beneficiam com uma estratégia de alocação. Para obter mais informações, consulte [Estratégias de alocação para Instâncias spot \(p. 733\)](#).

Usar uma EC2 Fleet do tipo 'instantâneo'

A EC2 Fleet do tipo instantâneo é uma solicitação síncrona única que faz apenas uma tentativa de iniciar a capacidade desejada. A resposta da API lista as instâncias que foram iniciadas juntamente com os erros das instâncias que não puderam ser iniciadas. Há vários benefícios de se usar uma EC2 Fleet do tipo Instantâneo, e eles são descritos neste artigo. Exemplos de configurações são fornecidos no fim do artigo.

Para workloads que precisam de uma API somente de inicialização para iniciar instâncias do EC2, você pode usar a API `RunInstances`. No entanto, com `RunInstances`, você só pode iniciar Instâncias sob demanda ou instâncias spot, mas não ambas na mesma solicitação. Além disso, quando você usa `RunInstances` para iniciar Instâncias spot, sua solicitação de Instância spot é limitada a um tipo de instância e a uma zona de disponibilidade. Isso visa um único grupo de capacidade spot (um conjunto de instâncias com o mesmo tipo de instância e zona de disponibilidade). Se o grupo de capacidade spot não tiver capacidade de instância spot suficiente para sua solicitação, a chamada `RunInstances` não tem sucesso.

Em vez de usar `RunInstances` para iniciar Instâncias spot, é recomendável usar a API `CreateFleet` com o parâmetro `type` definido como `instant` para obter os seguintes benefícios:

- Iniciar Instâncias sob demanda e instâncias spot em uma única solicitação. Uma EC2 Fleet pode iniciar Instâncias sob demanda, instâncias spot ou ambas. A solicitação das Instâncias spot é atendida se houver capacidade disponível e o preço máximo por hora para sua solicitação excede o preço Spot.
- Aumente a disponibilidade das instâncias spot. Usando uma EC2 Fleet do tipo `instant`, você pode iniciar instâncias spot seguindo as [Práticas recomendadas para spot](#) com os benefícios decorrentes disso:
 - Prática recomendada para spot: seja flexível sobre tipos de instância e zonas de disponibilidade.

Benefício: especificando vários tipos de instância e zonas de disponibilidade, você aumenta o número de grupos de capacidade spot. Isso dá ao serviço de spot uma chance maior de encontrar e alocar sua capacidade computacional spot desejada. Uma boa regra geral é ser flexível em pelo menos 10 tipos de instância para cada workload e garantir que todas as zonas de disponibilidade estejam configuradas para uso na sua VPC.

- Prática recomendada para spot: Use a estratégia de alocação otimizada para capacidade.

Benefício: a estratégia de alocação `capacity-optimized` provisiona automaticamente as instâncias a partir dos grupos de capacidade spot de maior disponibilidade. Como a capacidade de instâncias spot é proveniente de grupos com capacidade ideal, isso diminui a possibilidade de que as instâncias spot sejam interrompidas quando o Amazon EC2 precisar recuperar capacidade.

- Tenha acesso a um conjunto mais amplo de recursos. Para workloads que precisam de uma API somente de lançamento e em que você prefere gerenciar o ciclo de vida de sua instância em vez de deixar a frota EC2 gerenciá-lo para você, use a EC2 Fleet do tipo `instant` em vez da API `RunInstances`. A EC2 Fleet fornece um conjunto mais amplo de recursos do que o `RunInstances`, conforme demonstrado nos exemplos a seguir. Para todas as outras workloads, você deve usar o Amazon EC2 Auto Scaling, porque ele fornece um conjunto de recursos mais abrangente para uma grande variedade de workloads, como aplicativos apoiados pelo ELB, workloads em contêineres e trabalhos de processamento de fila.

Os serviços da AWS, como o Amazon EC2 Auto Scaling e o Amazon EMR, usam o tipo de EC2 Fleet instantâneo para iniciar instâncias do EC2.

Pré-requisitos para a EC2 Fleet do tipo instantâneo

Para obter os pré-requisitos para criar uma EC2 Fleet, consulte [Pré-requisitos da Frota do EC2 \(p. 743\)](#).

Como uma EC2 Fleet instantânea funciona

Ao trabalhar com uma EC2 Fleet do tipo `instant`, a sequência de eventos é a seguinte:

1. Configure o tipo de solicitação `CreateFleet` como `instant`. Para obter mais informações, consulte [Criar uma Frota do EC2. \(p. 751\)](#). Observe que, após fazer a chamada de API, você não pode modificá-la.
2. Quando você faz uma chamada de API, a EC2 Fleet faz uma solicitação síncrona única da capacidade desejada.
3. A resposta da API lista as instâncias que foram iniciadas juntamente com os erros das instâncias que não puderam ser iniciadas.
4. Você pode descrever a EC2 Fleet, listar as instâncias associadas à EC2 Fleet e visualizar o histórico da EC2 Fleet.
5. Depois que suas instâncias são iniciadas, você pode [excluir a solicitação de frota](#). Ao excluir a solicitação de frota, você também pode optar por encerrar as instâncias associadas ou deixá-las em execução.
6. É possível encerrar as instâncias a qualquer momento.

Examples

Os exemplos a seguir mostram como usar a EC2 Fleet do tipo `instant` para diferentes casos de uso. Para obter mais informações sobre como usar os parâmetros da API `CreateFleet` do EC2, consulte [Criar frota](#) na Referência de API do Amazon EC2.

Exemplos

- [Exemplo 1: Iniciar instâncias spot com a estratégia de alocação otimizada para capacidade \(p. 716\)](#)

- Exemplo 2: iniciar uma única instância spot com a estratégia de alocação otimizada para capacidade (p. 717)
- Exemplo 3: iniciar uma frota spot usando pesos de instâncias (p. 719)
- Exemplo 4: iniciar instâncias spot dentro de uma única zona de disponibilidade (p. 720)
- Exemplo 5: iniciar instâncias spot de um tipo de instância único dentro de uma única zona de disponibilidade (p. 721)
- Exemplo 6: iniciar instâncias spot somente se a capacidade mínima pretendida puder ser iniciada (p. 723)
- Exemplo 7: iniciar instâncias spot apenas se a capacidade mínima pretendida puder ser iniciada do mesmo tipo de instância em uma única zona de disponibilidade (p. 724)
- Exemplo 8: iniciar instâncias com vários modelos de lançamento (p. 725)
- Exemplo 9: iniciar instância spot com uma base de Instâncias sob demanda (p. 727)
- Exemplo 10: iniciar Instâncias spot usando uma estratégia de alocação otimizada para capacidade com uma base de Instâncias sob demanda usando Reservas de Capacidade e a estratégia de alocação priorizada (p. 728)
- Exemplo 11: iniciar Instâncias spot usando a estratégia de alocação capacity-optimized-prioritized (p. 731)

Exemplo 1: Iniciar instâncias spot com a estratégia de alocação otimizada para capacidade

O exemplo a seguir especifica os parâmetros mínimos necessários em uma EC2 Fleet do tipo `instant`: um modelo de lançamento, a capacidade pretendida, a opção de compra padrão e as substituições do modelo de lançamento.

- O modelo de lançamento é identificado por nome e número de versão do modelo de lançamento.
- As 12 substituições do modelo de lançamento especificam 4 tipos de instância diferentes e 3 sub-redes diferentes, cada uma em uma zona de disponibilidade separada. Cada combinação de tipo de instância e sub-rede define um grupo de capacidade spot, resultando em 12 pools de capacidade spot.
- A capacidade mínima pretendida para a frota é de 20 instâncias.
- A opção de compra padrão é `spot`, o que resulta na tentativa da frota de iniciar 20 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias que estão sendo iniciadas.

```
{  
    "SpotOptions": {  
        "AllocationStrategy": "capacity-optimized"  
    },  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification":{  
                "LaunchTemplateName":"ec2-fleet-lt1",  
                "Version": "$Latest"  
            },  
            "Overrides": [  
                {  
                    "InstanceType": "c5.large",  
                    "SubnetId": "subnet-fae8c380"  
                },  
                {  
                    "InstanceType": "c5.large",  
                    "SubnetId": "subnet-e7188bab"  
                },  
                {  
                    "InstanceType": "c5.large",  
                    "SubnetId": "subnet-49e41922"  
                }  
            ]  
        }  
    ]  
}
```

```
        },
        {
            "InstanceType": "c5d.large",
            "SubnetId": "subnet-fae8c380"
        },
        {
            "InstanceType": "c5d.large",
            "SubnetId": "subnet-e7188bab"
        },
        {
            "InstanceType": "c5d.large",
            "SubnetId": "subnet-49e41922"
        },
        {
            "InstanceType": "m5.large",
            "SubnetId": "subnet-fae8c380"
        },
        {
            "InstanceType": "m5.large",
            "SubnetId": "subnet-e7188bab"
        },
        {
            "InstanceType": "m5.large",
            "SubnetId": "subnet-49e41922"
        },
        {
            "InstanceType": "m5d.large",
            "SubnetId": "subnet-fae8c380"
        },
        {
            "InstanceType": "m5d.large",
            "SubnetId": "subnet-e7188bab"
        },
        {
            "InstanceType": "m5d.large",
            "SubnetId": "subnet-49e41922"
        }
    ]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemplo 2: iniciar uma única instância spot com a estratégia de alocação otimizada para capacidade

Você pode iniciar de forma ideal uma instância spot de cada vez fazendo várias chamadas de API da EC2 Fleet do tipo instant, definindo o TotalTargetCapacity como 1.

O exemplo a seguir especifica os parâmetros mínimos necessários em uma EC2 Fleet do tipo instantâneo: um modelo de lançamento, a capacidade pretendida, a opção de compra padrão e as substituições do modelo de lançamento. O modelo de lançamento é identificado por nome e número de versão do modelo de lançamento. As 12 substituições do modelo de lançamento têm 4 tipos de instância diferentes e 3 sub-redes diferentes, cada uma em uma zona de disponibilidade separada. A capacidade pretendida da frota é 1 instância, e a opção de compra padrão é spot, o que resulta na tentativa da frota de iniciar uma instância spot a partir de um dos 12 grupos de capacidade spot com base na estratégia de alocação otimizada para capacidade, para iniciar uma instância spot a partir do grupo de capacidade mais disponível.

```
{
```

```
"SpotOptions": {  
    "AllocationStrategy": "capacity-optimized"  
},  
"LaunchTemplateConfigs": [  
    {  
        "LaunchTemplateSpecification":{  
            "LaunchTemplateName":"ec2-fleet-lt1",  
            "Version": "$Latest"  
        },  
        "Overrides": [  
            {  
                "InstanceType": "c5.large",  
                "SubnetId": "subnet-fae8c380"  
            },  
            {  
                "InstanceType": "c5.large",  
                "SubnetId": "subnet-e7188bab"  
            },  
            {  
                "InstanceType": "c5.large",  
                "SubnetId": "subnet-49e41922"  
            },  
            {  
                "InstanceType": "c5d.large",  
                "SubnetId": "subnet-fae8c380"  
            },  
            {  
                "InstanceType": "c5d.large",  
                "SubnetId": "subnet-e7188bab"  
            },  
            {  
                "InstanceType": "c5d.large",  
                "SubnetId": "subnet-49e41922"  
            },  
            {  
                "InstanceType": "m5.large",  
                "SubnetId": "subnet-fae8c380"  
            },  
            {  
                "InstanceType": "m5.large",  
                "SubnetId": "subnet-e7188bab"  
            },  
            {  
                "InstanceType": "m5.large",  
                "SubnetId": "subnet-49e41922"  
            },  
            {  
                "InstanceType": "m5d.large",  
                "SubnetId": "subnet-fae8c380"  
            },  
            {  
                "InstanceType": "m5d.large",  
                "SubnetId": "subnet-e7188bab"  
            },  
            {  
                "InstanceType": "m5d.large",  
                "SubnetId": "subnet-49e41922"  
            }  
        ]  
    }  
],  
"TargetCapacitySpecification": {  
    "TotalTargetCapacity": 1,  
    "DefaultTargetCapacityType": "spot"  
},  
"Type": "instant"
```

}

Exemplo 3: iniciar uma frota spot usando pesos de instâncias

Os exemplos a seguir usam o peso da instância, o que significa que o preço é por hora em vez de ser por hora de instância. Cada configuração de execução lista um tipo de instância diferente e um peso diferente com base em quantas unidades da workload podem ser executadas na instância, pressupondo que uma unidade da workload requeira 15 GB de memória e 4 vCPUs. Por exemplo, m5.xlarge (4 vCPUs e 16 GB de memória) pode executar uma unidade e tem peso 1, m5.2xlarge (8 vCPUs e 32 GB de memória) pode executar 2 unidades e tem peso 2, e assim por diante. A capacidade total pretendida é definida como 40 unidades. A opção de compra padrão é spot, e a estratégia de alocação é otimizada para capacidade, o que resulta em 40 m5.xlarge (40 dividido por 1), 20 m5.2xlarge (40 dividido por 2), 10 m5.4xlarge (40 dividido por 4), 5 m5.8xlarge (40 dividido por 8) ou uma combinação de tipos de instância com pesos que somam a capacidade desejada com base na estratégia de alocação otimizada para capacidade.

Para obter mais informações, consulte [Peso de instâncias da Frota do EC2 \(p. 740\)](#).

```
{  
    "SpotOptions":{  
        "AllocationStrategy":"capacity-optimized"  
    },  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification":{  
                "LaunchTemplateName":"ec2-fleet-lt1",  
                "Version":"$Latest"  
            },  
            "Overrides": [  
                {  
                    "InstanceType":"m5.xlarge",  
                    "SubnetId":"subnet-fae8c380",  
                    "WeightedCapacity":1  
                },  
                {  
                    "InstanceType":"m5.xlarge",  
                    "SubnetId":"subnet-e7188bab",  
                    "WeightedCapacity":1  
                },  
                {  
                    "InstanceType":"m5.xlarge",  
                    "SubnetId":"subnet-49e41922",  
                    "WeightedCapacity":1  
                },  
                {  
                    "InstanceType":"m5.2xlarge",  
                    "SubnetId":"subnet-fae8c380",  
                    "WeightedCapacity":2  
                },  
                {  
                    "InstanceType":"m5.2xlarge",  
                    "SubnetId":"subnet-e7188bab",  
                    "WeightedCapacity":2  
                },  
                {  
                    "InstanceType":"m5.2xlarge",  
                    "SubnetId":"subnet-49e41922",  
                    "WeightedCapacity":2  
                },  
                {  
                    "InstanceType":"m5.4xlarge",  
                    "SubnetId":"subnet-fae8c380",  
                    "WeightedCapacity":4  
                },  
            ]  
        }  
    ]  
}
```

```
{  
    "InstanceType": "m5.4xlarge",  
    "SubnetId": "subnet-e7188bab",  
    "WeightedCapacity": 4  
},  
{  
    "InstanceType": "m5.4xlarge",  
    "SubnetId": "subnet-49e41922",  
    "WeightedCapacity": 4  
},  
{  
    "InstanceType": "m5.8xlarge",  
    "SubnetId": "subnet-fae8c380",  
    "WeightedCapacity": 8  
},  
{  
    "InstanceType": "m5.8xlarge",  
    "SubnetId": "subnet-e7188bab",  
    "WeightedCapacity": 8  
},  
{  
    "InstanceType": "m5.8xlarge",  
    "SubnetId": "subnet-49e41922",  
    "WeightedCapacity": 8  
}  
]  
]  
],  
"TargetCapacitySpecification": {  
    "TotalTargetCapacity": 40,  
    "DefaultTargetCapacityType": "spot"  
},  
"Type": "instant"  
}
```

Exemplo 4: iniciar instâncias spot dentro de uma única zona de disponibilidade

Você pode configurar uma frota para iniciar todas as instâncias em uma única zona de disponibilidade definindo as opções de spot SingleAvailabilityZone como true.

As 12 substituições do modelo de lançamento têm tipos de instância e sub-redes diferentes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida é de 20 instâncias, a opção de compra padrão é spot e a estratégia de alocação spot é otimizada para capacidade. A EC2 Fleet inicia 20 instâncias spot, todas em uma única AZ, a partir dos grupos de capacidade spot com capacidade ideal usando as especificações de lançamento.

```
{  
    "SpotOptions": {  
        "AllocationStrategy": "capacity-optimized",  
        "SingleAvailabilityZone": true  
    },  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateName": "ec2-fleet-lt1",  
                "Version": "$Latest"  
            },  
            "Overrides": [  
                {  
                    "InstanceType": "c5.4xlarge",  
                    "SubnetId": "subnet-fae8c380"  
                },  
                {  
                    "InstanceType": "c5.8xlarge",  
                    "SubnetId": "subnet-49e41922"  
                }  
            ]  
        }  
    ]  
}
```

```
        "InstanceType": "c5.4xlarge",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "c5.4xlarge",
        "SubnetId": "subnet-49e41922"
    },
    {
        "InstanceType": "c5d.4xlarge",
        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "c5d.4xlarge",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "c5d.4xlarge",
        "SubnetId": "subnet-49e41922"
    },
    {
        "InstanceType": "m5.4xlarge",
        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "m5.4xlarge",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5.4xlarge",
        "SubnetId": "subnet-49e41922"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-49e41922"
    }
]
}
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemplo 5: iniciar instâncias spot de um tipo de instância único dentro de uma única zona de disponibilidade

Você pode configurar uma frota para iniciar todas as instâncias do mesmo tipo de instância em uma única zona de disponibilidade definindo SpotOptions SingleInstanceType como true e SingleAvailabilityZone como true.

As 12 substituições do modelo de lançamento têm tipos de instância e sub-redes diferentes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida é de 20 instâncias, a opção de compra padrão é spot e a estratégia de alocação spot é otimizada para capacidade. A EC2 Fleet inicia 20 instâncias spot do mesmo tipo de instância, todas em

uma única AZ, a partir do grupo de capacidade spot com capacidade ideal usando as especificações de lançamento.

```
{  
    "SpotOptions": {  
        "AllocationStrategy": "capacity-optimized",  
        "SingleInstanceType": true,  
        "SingleAvailabilityZone": true  
    },  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification":{  
                "LaunchTemplateName":"ec2-fleet-lt1",  
                "Version":"$Latest"  
            },  
            "Overrides": [  
                {  
                    "InstanceType":"c5.4xlarge",  
                    "SubnetId":"subnet-fae8c380"  
                },  
                {  
                    "InstanceType":"c5.4xlarge",  
                    "SubnetId":"subnet-e7188bab"  
                },  
                {  
                    "InstanceType":"c5.4xlarge",  
                    "SubnetId":"subnet-49e41922"  
                },  
                {  
                    "InstanceType":"c5d.4xlarge",  
                    "SubnetId":"subnet-fae8c380"  
                },  
                {  
                    "InstanceType":"c5d.4xlarge",  
                    "SubnetId":"subnet-e7188bab"  
                },  
                {  
                    "InstanceType":"c5d.4xlarge",  
                    "SubnetId":"subnet-49e41922"  
                },  
                {  
                    "InstanceType":"m5.4xlarge",  
                    "SubnetId":"subnet-fae8c380"  
                },  
                {  
                    "InstanceType":"m5.4xlarge",  
                    "SubnetId":"subnet-e7188bab"  
                },  
                {  
                    "InstanceType":"m5.4xlarge",  
                    "SubnetId":"subnet-49e41922"  
                },  
                {  
                    "InstanceType":"m5d.4xlarge",  
                    "SubnetId":"subnet-fae8c380"  
                },  
                {  
                    "InstanceType":"m5d.4xlarge",  
                    "SubnetId":"subnet-e7188bab"  
                },  
                {  
                    "InstanceType":"m5d.4xlarge",  
                    "SubnetId":"subnet-49e41922"  
                }  
            ]  
        }  
    ]  
}
```

```
        },
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Exemplo 6: iniciar instâncias spot somente se a capacidade mínima pretendida puder ser iniciada

Você pode configurar uma frota para iniciar as instâncias somente se a capacidade mínima pretendida puder ser iniciada, definindo as opções de spot MinTargetCapacity como a capacidade pretendida que você deseja iniciar em conjunto.

As 12 substituições do modelo de lançamento têm tipos de instância e sub-redes diferentes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida e a capacidade mínima pretendida são ambas definidas como 20 instâncias, a opção de compra padrão é spot e a estratégia de alocação spot é otimizada para capacidade. A Frota do EC2 inicia 20 instâncias spot a partir do grupo de capacidade spot com capacidade ideal usando as substituições do modelo de lançamento, apenas se puder iniciar todas as 20 instâncias ao mesmo tempo.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "ec2-fleet-lt1",
                "Version": "$Latest"
            },
            "Overrides": [
                {
                    "InstanceType": "c5.4xlarge",
                    "SubnetId": "subnet-fae8c380"
                },
                {
                    "InstanceType": "c5.4xlarge",
                    "SubnetId": "subnet-e7188bab"
                },
                {
                    "InstanceType": "c5.4xlarge",
                    "SubnetId": "subnet-49e41922"
                },
                {
                    "InstanceType": "c5d.4xlarge",
                    "SubnetId": "subnet-fae8c380"
                },
                {
                    "InstanceType": "c5d.4xlarge",
                    "SubnetId": "subnet-e7188bab"
                },
                {
                    "InstanceType": "c5d.4xlarge",
                    "SubnetId": "subnet-49e41922"
                },
                {
                    "InstanceType": "m5.4xlarge",
                    "SubnetId": "subnet-fae8c380"
                },
                {
                    "InstanceType": "m5.4xlarge",

```

```
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5.4xlarge",
        "SubnetId": "subnet-49e41922"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5d.4xlarge",
        "SubnetId": "subnet-49e41922"
    }
]
},
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemplo 7: iniciar instâncias spot apenas se a capacidade mínima pretendida puder ser iniciada do mesmo tipo de instância em uma única zona de disponibilidade

Você pode configurar uma frota para iniciar as instâncias apenas se a capacidade mínima pretendida puder ser iniciada com um único tipo de instância em uma única zona de disponibilidade, definindo as opções de spot MinTargetCapacity como a capacidade mínima pretendida que você deseja iniciar ao mesmo tempo, juntamente com as opções SingleInstanceType e SingleAvailabilityZone.

As 12 especificações que substituem o modelo de lançamento têm diferentes tipos de instância e sub-redes (cada uma em uma zona de disponibilidade separada), mas a mesma capacidade ponderada. A capacidade total pretendida e a capacidade mínima pretendida são ambas definidas como 20 instâncias, a opção de compra padrão é spot, a estratégia de alocação spot é otimizada para capacidade, SingleInstanceType é true e SingleAvailabilityZone é true. A EC2 Fleet inicia 20 instâncias spot, todas do mesmo tipo de instância e todas em uma única AZ, a partir do grupo de capacidade spot com capacidade ideal usando as especificações de lançamento, apenas se puder iniciar todas as 20 instâncias ao mesmo tempo.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "ec2-fleet-lt1",
                "Version": "$Latest"
            },
            "Overrides": [
                {
                    "InstanceType": "c5.4xlarge",
                    "SubnetId": "subnet-fae8c380"
                },
                {
                    "InstanceType": "m5.4xlarge",
                    "SubnetId": "subnet-e7188bab"
                }
            ]
        }
    ]
}
```

```
{  
    "InstanceType": "c5.4xlarge",  
    "SubnetId": "subnet-e7188bab"  
},  
{  
    "InstanceType": "c5.4xlarge",  
    "SubnetId": "subnet-49e41922"  
},  
{  
    "InstanceType": "c5d.4xlarge",  
    "SubnetId": "subnet-fae8c380"  
},  
{  
    "InstanceType": "c5d.4xlarge",  
    "SubnetId": "subnet-e7188bab"  
},  
{  
    "InstanceType": "c5d.4xlarge",  
    "SubnetId": "subnet-49e41922"  
},  
{  
    "InstanceType": "m5.4xlarge",  
    "SubnetId": "subnet-fae8c380"  
},  
{  
    "InstanceType": "m5.4xlarge",  
    "SubnetId": "subnet-e7188bab"  
},  
{  
    "InstanceType": "m5.4xlarge",  
    "SubnetId": "subnet-49e41922"  
},  
{  
    "InstanceType": "m5d.4xlarge",  
    "SubnetId": "subnet-fae8c380"  
},  
{  
    "InstanceType": "m5d.4xlarge",  
    "SubnetId": "subnet-e7188bab"  
},  
{  
    "InstanceType": "m5d.4xlarge",  
    "SubnetId": "subnet-49e41922"  
}  
]  
}  
],  
"TargetCapacitySpecification": {  
    "TotalTargetCapacity": 20,  
    "DefaultTargetCapacityType": "spot"  
},  
"Type": "instant"  
}
```

Exemplo 8: iniciar instâncias com vários modelos de lançamento

Você pode configurar uma frota para iniciar instâncias com diferentes especificações de lançamento para diferentes tipos de instância ou um grupo de tipos de instância, especificando vários modelos de lançamento. Neste exemplo, queremos ter diferentes tamanhos de volume do EBS para diferentes tipos de instância e temos isso configurado nos modelos de lançamento ec2-fleet-lt-4xl, ec2-fleet-lt-9xl e ec2-fleet-lt-18xl.

Neste exemplo, usaremos 3 modelos de lançamento diferentes para os 3 tipos de instância, com base em seu tamanho. As especificação de lançamento faz a substituição em todos os modelos de lançamento

que usam pesos de instância com base nas vCPUs no tipo de instância. A capacidade total pretendida é de 144 instâncias, a opção de compra padrão é spot e a estratégia de alocação de spot é otimizada para capacidade. A EC2 Fleet pode iniciar 9 c5n.4xlarge (144 dividido por 16) usando o modelo de lançamento ec2-fleet-4xl, ou 4 c5n.9xlarge (144 dividido por 36), usando o modelo de lançamento ec2-fleet-9xl, ou 2 c5n.18xlarge (144 dividido por 72), usando o modelo de lançamento ec2-fleet-18xl, ou uma combinação dos tipos de instância com pesos que somam a capacidade desejada com base na estratégia de alocação otimizada para capacidade.

```
{  
    "SpotOptions": {  
        "AllocationStrategy": "capacity-optimized"  
    },  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification":{  
                "LaunchTemplateName":"ec2-fleet-lt-18xl",  
                "Version":"$Latest"  
            },  
            "Overrides": [  
                {  
                    "InstanceType":"c5n.18xlarge",  
                    "SubnetId":"subnet-fae8c380",  
                    "WeightedCapacity":72  
                },  
                {  
                    "InstanceType":"c5n.18xlarge",  
                    "SubnetId":"subnet-e7188bab",  
                    "WeightedCapacity":72  
                },  
                {  
                    "InstanceType":"c5n.18xlarge",  
                    "SubnetId":"subnet-49e41922",  
                    "WeightedCapacity":72  
                }  
            ]  
        },  
        {  
            "LaunchTemplateSpecification":{  
                "LaunchTemplateName":"ec2-fleet-lt-9xl",  
                "Version":"$Latest"  
            },  
            "Overrides": [  
                {  
                    "InstanceType":"c5n.9xlarge",  
                    "SubnetId":"subnet-fae8c380",  
                    "WeightedCapacity":36  
                },  
                {  
                    "InstanceType":"c5n.9xlarge",  
                    "SubnetId":"subnet-e7188bab",  
                    "WeightedCapacity":36  
                },  
                {  
                    "InstanceType":"c5n.9xlarge",  
                    "SubnetId":"subnet-49e41922",  
                    "WeightedCapacity":36  
                }  
            ]  
        },  
        {  
            "LaunchTemplateSpecification":{  
                "LaunchTemplateName":"ec2-fleet-lt-4xl",  
                "Version":"$Latest"  
            },  
    ]  
}
```

```
"Overrides": [
    {
        "InstanceType": "c5n.4xlarge",
        "SubnetId": "subnet-fae8c380",
        "WeightedCapacity": 16
    },
    {
        "InstanceType": "c5n.4xlarge",
        "SubnetId": "subnet-e7188bab",
        "WeightedCapacity": 16
    },
    {
        "InstanceType": "c5n.4xlarge",
        "SubnetId": "subnet-49e41922",
        "WeightedCapacity": 16
    }
]
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 144,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemplo 9: iniciar instância spot com uma base de Instâncias sob demanda

O exemplo a seguir especifica a capacidade total pretendida de 20 instâncias para a frota e uma capacidade pretendida de 5 Instâncias sob demanda. A opção de compra padrão é spot. A frota inicia 5 Instâncias sob demanda, conforme especificado, mas precisa iniciar mais 15 instâncias para atender à capacidade total pretendida. A opção de compra para a diferença é calculada como TotalTargetCapacity – OnDemandTargetCapacity = DefaultTargetCapacityType, que resulta no lançamento pela frota de 15 Instâncias spot a partir de um dos 12 grupos de capacidade de spot com base na estratégia de alocação otimizada para capacidade.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "ec2-fleet-lt1",
                "Version": "$Latest"
            },
            "Overrides": [
                {
                    "InstanceType": "c5.large",
                    "SubnetId": "subnet-fae8c380"
                },
                {
                    "InstanceType": "c5.large",
                    "SubnetId": "subnet-e7188bab"
                },
                {
                    "InstanceType": "c5.large",
                    "SubnetId": "subnet-49e41922"
                },
                {
                    "InstanceType": "c5d.large",
                    "SubnetId": "subnet-fae8c380"
                },
                {

```

```
        "InstanceType": "c5d.large",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "c5d.large",
        "SubnetId": "subnet-49e41922"
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-49e41922"
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-fae8c380"
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-e7188bab"
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-49e41922"
    }
]
},
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "OnDemandTargetCapacity": 5,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Exemplo 10: iniciar Instâncias spot usando uma estratégia de alocação otimizada para capacidade com uma base de Instâncias sob demanda usando Reservas de Capacidade e a estratégia de alocação priorizada

É possível configurar uma frota para usar Reservas de Capacidade sob demanda primeiro ao iniciar Instâncias sob demanda com o tipo de capacidade pretendida padrão como spot, definindo a estratégia de uso para Reservas de Capacidade como use-capacity-reservations-first. E se vários grupos de instâncias tiverem Reservas de Capacidade não utilizadas, a estratégia de alocação sob demanda escolhida será aplicada. Neste exemplo, a estratégia de alocação sob demanda é priorizada.

Neste exemplo, há 6 Reservas de Capacidade não utilizadas disponíveis. Isso é menos que a capacidade sob demanda pretendida da frota de 10 Instâncias sob demanda.

A conta tem as seguintes 6 Reservas de Capacidade não utilizadas em 2 grupos diferentes. O número de Reservas de Capacidade em cada grupo é indicado por AvailableInstanceCount.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
```

```
        "AvailableInstanceCount": 3,
        "InstanceMatchCriteria": "open",
        "State": "active"
    }
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A estratégia de alocação sob demanda é priorizada, e a estratégia de uso para Reservas de Capacidade é use-capacity-reservations-first. A estratégia de alocação spot é otimizada para capacidade. A capacidade total pretendida é de 20, a capacidade sob demanda pretendida é de 10 e o tipo de capacidade pretendida padrão é spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions": {
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "AllocationStrategy": "prioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "ec2-fleet-lt1",
                "Version": "$Latest"
            },
            "Overrides": [
                {
                    "InstanceType": "c5.large",
                    "SubnetId": "subnet-fae8c380",
                    "Priority": 1.0
                },
                {
                    "InstanceType": "c5.large",
                    "SubnetId": "subnet-e7188bab",
                    "Priority": 2.0
                },
                {
                    "InstanceType": "c5.large",
                    "SubnetId": "subnet-49e41922",
                    "Priority": 3.0
                },
                {
                    "InstanceType": "c5d.large",
                    "SubnetId": "subnet-fae8c380",
                    "Priority": 4.0
                },
                {
                    "InstanceType": "c5d.large",
                    "SubnetId": "subnet-e7188bab",
                    "Priority": 5.0
                }
            ]
        }
    ]
}
```

```
        "InstanceType": "c5d.large",
        "SubnetId": "subnet-49e41922",
        "Priority": 6.0
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-fae8c380",
        "Priority": 7.0
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-e7188bab",
        "Priority": 8.0
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-49e41922",
        "Priority": 9.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-fae8c380",
        "Priority": 10.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-e7188bab",
        "Priority": 11.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-49e41922",
        "Priority": 12.0
    }
]
},
],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 20,
    "OnDemandTargetCapacity": 10,
    "DefaultTargetCapacityType": "spot"
},
"Type": "instant"
}
```

Depois de criar a frota instantânea usando a configuração anterior, as 20 instâncias a seguir serão iniciadas para atender à capacidade pretendida:

- 7 Instâncias sob demanda c5.large em us-east-1a – c5.large em us-east-1a é priorizada, e há 3 Reservas de Capacidade c5.large não utilizadas disponíveis. As Reservas de Capacidade são usadas primeiro para iniciar 3 Instâncias sob demanda, e 4 Instâncias sob demanda adicionais são iniciadas de acordo com a estratégia de alocação sob demanda, que é priorizada neste exemplo.
- 3 Instâncias sob demanda m5.large em us-east-1a – m5.large em us-east-1a é priorizada em segundo lugar, e há 3 Reservas de Capacidade c3.large não utilizadas disponíveis
- 10 instâncias spot a partir de um dos 12 grupos de capacidade spot que tem a capacidade ideal, de acordo com a estratégia de alocação otimizada para capacidade.

Depois que a frota for lançada, você poderá executar [describe-capacity-reservations](#) para ver quantas Reservas de Capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade de c5.large e m5.large foram usadas.

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "m5.large",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "c5.large",  
    "AvailableInstanceCount": 0  
}
```

Exemplo 11: iniciar Instâncias spot usando a estratégia de alocação capacity-optimized-prioritized

O exemplo a seguir especifica os parâmetros mínimos necessários em uma EC2 Fleet do tipo instantâneo: um modelo de lançamento, a capacidade pretendida, a opção de compra padrão e as substituições do modelo de lançamento. O modelo de lançamento é identificado por nome e número de versão do modelo de lançamento. As 12 especificações que substituem o modelo de lançamento têm 4 tipos de instância diferentes com uma prioridade atribuída e 3 sub-redes diferentes, cada uma em uma zona de disponibilidade separada. A capacidade pretendida para a frota é de 20 instâncias, e a opção de compra padrão é spot, o que resulta na tentativa da frota de iniciar 20 instâncias spot a partir de um dos 12 grupos de capacidade spot com base na estratégia de alocação capacity-optimized-prioritized, que tenta ao máximo implementar as prioridades, mas otimiza a capacidade em primeiro lugar.

```
{  
    "SpotOptions": {  
        "AllocationStrategy": "capacity-optimized-prioritized"  
    },  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification":{  
                "LaunchTemplateName":"ec2-fleet-lt1",  
                "Version": "$Latest"  
            },  
            "Overrides": [  
                {  
                    "InstanceType": "c5.large",  
                    "SubnetId": "subnet-fae8c380",  
                    "Priority": 1.0  
                },  
                {  
                    "InstanceType": "c5.large",  
                    "SubnetId": "subnet-e7188bab",  
                    "Priority": 1.0  
                },  
                {  
                    "InstanceType": "c5.large",  
                    "SubnetId": "subnet-49e41922",  
                    "Priority": 1.0  
                },  
                {  
                    "InstanceType": "c5d.large",  
                    "SubnetId": "subnet-fae8c380",  
                    "Priority": 2.0  
                },  
                {  
                    "InstanceType": "c5d.large",  
                    "SubnetId": "subnet-e7188bab",  
                    "Priority": 2.0  
                },  
                {  
                    "InstanceType": "c5d.large",  
                    "SubnetId": "subnet-49e41922",  
                    "Priority": 2.0  
                }  
            ]  
        }  
    ]  
}
```

```
        "Priority": 2.0
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-fae8c380",
        "Priority": 3.0
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-e7188bab",
        "Priority": 3.0
    },
    {
        "InstanceType": "m5.large",
        "SubnetId": "subnet-49e41922",
        "Priority": 3.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-fae8c380",
        "Priority": 4.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-e7188bab",
        "Priority": 4.0
    },
    {
        "InstanceType": "m5d.large",
        "SubnetId": "subnet-49e41922",
        "Priority": 4.0
    }
]
},
{
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Estratégias de configuração da Frota do EC2

Uma Frota do EC2 é um grupo de Instâncias on-demand e Instâncias spot.

A Frota do EC2 tenta executar o número de instâncias necessárias para atender à capacidade de destino especificada na solicitação de frota. A frota pode incluir somente Instâncias on-demand, somente Instâncias spot ou uma combinação de Instâncias on-demand e Instâncias spot. A solicitação das Instâncias spot é atendida se houver capacidade disponível e o preço máximo por hora para sua solicitação excede o preço Spot. A frota também tenta manter sua capacidade alvo caso as Instâncias spot sejam interrompidas.

Você também poderá definir um valor máximo por hora que esteja disposto a pagar pela frota, e o Frota do EC2 executará instâncias até alcançar o valor máximo. Quando o valor máximo que você está disposto a pagar for alcançado, a frota interromperá a execução de instâncias mesmo que a capacidade de destino ainda não tenha sido alcançada.

Um Grupo de capacidade spot é um conjunto de instâncias do EC2 não utilizadas, com o mesmo tipo de instância e zona de disponibilidade. Ao criar uma Frota do EC2, você poderá incluir várias especificações de execução, que variam de acordo com o tipo de instância, a zona de disponibilidade, a sub-rede e o preço máximo. A frota seleciona os grupos de capacidade spot que são usados para atender à solicitação

com base nas especificações de execução incluídas na sua solicitação e na configuração da solicitação. As Instâncias spot vêm dos grupos selecionados.

Com uma Frota do EC2, é possível provisionar muita capacidade do EC2. Isso é uma vantagem para aplicações com base no número de núcleos/instâncias ou na quantidade de memória. Por exemplo, você pode especificar uma Frota do EC2 para executar uma capacidade de destino de 200 instâncias, das quais 130 serão Instâncias on-demand e o restante Instâncias spot.

Use as estratégias de configuração apropriadas para criar uma Frota do EC2 que atenda às suas necessidades.

Tópicos

- [Planejar uma EC2 Fleet \(p. 733\)](#)
- [Estratégias de alocação para Instâncias spot \(p. 733\)](#)
- [Configurar Frota do EC2 para backup sob demanda \(p. 736\)](#)
- [Rebalanceamento de capacidade \(p. 737\)](#)
- [Sobreposições de preço máximo \(p. 739\)](#)
- [Controle de gastos \(p. 739\)](#)
- [Peso de instâncias da Frota do EC2 \(p. 740\)](#)

Planejar uma EC2 Fleet

Ao planejar sua Frota do EC2, recomendamos que você faça o seguinte:

- Determine se você deseja criar uma Frota do EC2 que envie uma solicitação síncrona ou assíncrona única da capacidade de destino desejada ou uma que mantenha uma capacidade de destino ao longo do tempo. Para obter mais informações, consulte [Tipos de solicitação da Frota do EC2 \(p. 714\)](#).
- Determine os tipos de instâncias que atendem aos requisitos da aplicação.
- Se você pretende incluir Instâncias spot na sua Frota do EC2, reveja as [Melhores práticas de spot](#) antes de criar a frota. Use essas melhores práticas ao planejar sua frota para que você possa provisionar as instâncias com o menor preço possível.
- Determine a capacidade de destino da sua Frota do EC2. Você pode definir a capacidade de destino em instâncias ou em unidades personalizadas. Para obter mais informações, consulte [Peso de instâncias da Frota do EC2 \(p. 740\)](#).
- Determine a parte da capacidade de destino da Frota do EC2 que deve ser de capacidade sob demanda e spot. Você pode especificar 0 para a capacidade sob demanda, a capacidade spot ou ambas.
- Determine seu preço por unidade, se você estiver usando o peso de instância. Para calcular o preço por unidade, divida o preço por hora de instância pelo número de unidades (ou peso) que essa instância representa. Se você não estiver usando o peso de instância, o preço padrão por unidade será o preço por hora de instância.
- Determine a quantidade máxima por hora que você está disposto a pagar pela sua frota. Para obter mais informações, consulte [Controle de gastos \(p. 739\)](#).
- Leia as opções possíveis para sua Frota do EC2. Para mais informações, consulte o [Referência do arquivo de configuração JSON da Frota do EC2 \(p. 747\)](#). Para exemplos de configuração da Frota do EC2, consulte [Exemplos de configuração de Frota do EC2 \(p. 824\)](#).

Estratégias de alocação para Instâncias spot

A estratégia de alocação da Frota do EC2 determina como ela atenderá à solicitação de Instâncias spot dos grupos de capacidade spot possíveis representados por suas especificações de execução. Veja a seguir as estratégias de alocação que você pode especificar na sua frota:

`lowest-price`

O Instâncias spot vêm do grupo de capacidade spot com o menor preço. Essa é a estratégia padrão.
`diversified`

Os Instâncias spot são distribuídos em todos os grupos de capacidade spot.
`capacity-optimized`

O Instâncias spot provém do grupo de capacidade spot com a capacidade ideal para o número de instâncias em execução. Opcionalmente, você pode definir uma prioridade para cada tipo de instância na frota usando o `capacity-optimized-prioritized`. A EC2 Fleet otimiza a capacidade primeiro, mas empenha-se em honrar as prioridades de tipo de instância.

Com as Instâncias spot, a definição de preço muda lentamente ao longo do tempo com base em tendências de longo prazo na oferta e na demanda, mas a capacidade oscila em tempo real. A estratégia `capacity-optimized` executa Instâncias spot automaticamente nos grupos mais disponíveis observando dados de capacidade em tempo real e prevendo quais são os mais disponíveis. Isso funciona bem para workloads, como big data e análise, renderização de imagens e mídia, machine learning e computação de alta performance, que podem ter um custo de interrupção maior associado ao reinício do trabalho e ao ponto de verificação. Ao oferecer a possibilidade de menos interrupções, a estratégia `capacity-optimized` pode reduzir o custo geral da workload.

Como alternativa, você pode usar a estratégia de alocação `capacity-optimized-prioritized` com um parâmetro de prioridade para ordenar os tipos de instância, da prioridade mais alta para a mais baixa. Você pode definir a mesma prioridade para diferentes tipos de instância. A EC2 Fleet otimizará a capacidade primeiro, mas se empenhará em honrar as prioridades de tipo de instância (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da EC2 Fleet de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante. Só haverá suporte para o uso de prioridades se a frota usar um modelo de lançamento. Observe que quando você define a prioridade para `capacity-optimized-prioritized`, a mesma prioridade também será aplicada às instâncias sob demanda se o `AllocationStrategy` sob demanda estiver definido como `prioritized`.

`InstancePoolsToUseCount`

As Instâncias spot são distribuídas pelo número de grupos de capacidade spot que você especificar. Este parâmetro é válido somente quando usado em combinação com `lowest-price`.

Manter a capacidade de destino

Depois que as Instâncias spot são encerradas devido a uma alteração no preço spot ou na capacidade disponível de um grupo de capacidade spot, uma Frota do EC2 do tipo `maintain` executa a substituição de Instâncias spot. Se a estratégia de alocação for `lowest-price`, a frota executará instâncias de substituição no grupo onde o preço spot for atualmente o menor. Se a estratégia de alocação for `lowest-price` combinada com `InstancePoolsToUseCount`, a frota selecionará os grupos de capacidade spot com o menor preço e lançará as Instâncias spot no número de grupos de capacidade spot que você especificar. Se a estratégia de alocação for `capacity-optimized`, a frota executará instâncias de substituição no grupo com a maior capacidade de instâncias spot disponível. Se a estratégia de alocação for `diversified`, a frota distribuirá as Instâncias spot de substituição pelos grupos restantes.

Escolher a estratégia de alocação apropriada

Você pode otimizar a frota com base no seu caso de uso.

Se a sua frota executar workloads que possam ter um custo maior de interrupção associado ao reinício de trabalho e ao ponto de verificação, use a estratégia `capacity-optimized`. Essa estratégia oferece a possibilidade de menos interrupções, o que pode reduzir o custo geral da workload. Use a estratégia

capacity-optimized-prioritized para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante.

Se a frota for pequena ou for executada por um período curto, a probabilidade de que as Instâncias spot sejam interrompidas será baixa, mesmo que todas as instâncias sejam de um único grupo de capacidade spot. Portanto, é provável que a estratégia lowest-price atenda às suas necessidades enquanto oferece o menor custo.

Se sua frota for grande ou estiver sendo executada há muito tempo, você poderá aprimorar a disponibilidade dela distribuindo as Instâncias spot por vários grupos, usando a estratégia diversified. Por exemplo, se a Frota do EC2 especificar 10 grupos e uma capacidade de destino de 100 instâncias, a frota executará 10 Instâncias spot em cada grupo. Se o preço spot para um grupo exceder seu preço máximo para esse mesmo grupo, somente 10% de sua frota será afetada. Usar essa estratégia também torna sua frota menos sensível a aumentos que ocorram com o tempo no preço spot em qualquer grupo específico. Com a estratégia diversified, a Frota do EC2 não executará Instâncias spot em nenhum grupo com um preço spot igual ou maior que o [preço sob demanda](#).

Para criar uma frota econômica e diversificada, use a estratégia lowest-price em combinação com `InstancePoolsToUseCount`. Você pode usar um número baixo ou alto de grupos de capacidade spot para alocar suas Instâncias spot. Por exemplo, se você executar o processamento em lote, recomendamos que especifique um número baixo de grupos de capacidade spot (por exemplo, `InstancePoolsToUseCount=2`) para garantir que sua fila sempre tenha capacidade computacional e otimize a economia. Se você executa um serviço Web, recomendamos que especifique um grande número de grupos de capacidade spot (por exemplo, `InstancePoolsToUseCount=10`) para minimizar o impacto se um grupo de capacidade spot ficar temporariamente indisponível.

Configurar Frota do EC2 para otimização de custos

Para otimizar os custos de uso de Instâncias spot, especifique a estratégia de alocação `lowest-price` de modo que a Frota do EC2 implante a combinação mais econômica de tipos de instância e zonas de disponibilidade de maneira automática e com base no preço spot atual.

Para a capacidade de destino de instância sob demanda, a Frota do EC2 sempre seleciona o tipo de instância mais barato com base no preço público sob demanda e continua seguindo a estratégia de alocação (`lowest-price`, `capacity-optimized` ou `diversified`) para Instâncias spot.

Configurar a Frota do EC2 para otimização de custos e diversificação

Para criar uma frota de instâncias spot econômica e diversificada, use a estratégia de alocação `lowest-price` em combinação com `InstancePoolsToUseCount`. A EC2 Fleet implanta a combinação mais barata de tipos de instância e zonas de disponibilidade de maneira automática e com base no preço spot atual no número de grupos de capacidade spot especificado. Esta combinação pode ser usada para evitar as Instâncias spot mais caras.

Por exemplo, se a capacidade de destino for 10 Instâncias Spot e você especificar 2 pools de capacidade spot (para `InstancePoolsToUseCount`), o EC2 Fleet utilizará os dois pools mais baratos para atender à sua capacidade spot.

Observe que o EC2 Fleet tenta extrair instâncias spot a partir do número de pools que você especificar com base no melhor esforço. Se um pool ficar sem capacidade spot antes de cumprir sua capacidade de destino, o EC2 Fleet continuará atendendo sua solicitação usando o próximo pool mais barato. Para garantir que sua capacidade de destino seja atendida, você pode receber Instâncias Spot de mais do que o número de pools especificado. Da mesma forma, se a maioria dos pools não tiver capacidade spot, você poderá receber sua capacidade de destino total de menos do que o número de pools que você especificou.

Configurar a Frota do EC2 para otimização de capacidade

Para iniciar instâncias spot nos grupos de capacidade spot mais disponíveis, use a estratégia de alocação `capacity-optimized`. Para obter uma configuração de exemplo, consulte [Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade](#) (p. 835).

Também é possível expressar as prioridades de seu grupo usando a estratégia de alocação `capacity-optimized-prioritized` e definir a ordem dos tipos de instância a serem usados, da prioridade mais alta para a mais baixa. Só haverá suporte para o uso de prioridades se a frota usar um modelo de lançamento. Observe que quando você define as prioridades para `capacity-optimized-prioritized`, as mesmas prioridades também serão aplicadas às instâncias sob demanda se o `AllocationStrategy` sob demanda estiver definido como `prioritized`. Para obter uma configuração de exemplo, consulte [Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades \(p. 836\)](#).

Configurar Frota do EC2 para backup sob demanda

Se houver a necessidade de escalas urgentes e imprevisíveis, como um site de notícias que deve ser dimensionado durante um grande evento de notícias ou execução de um jogo, recomendamos que você especifique tipos alternativos de instâncias para suas Instâncias on-demand, caso sua opção preferida não tenha capacidade disponível suficiente. Por exemplo, você pode preferir `c5.2xlarge` Instâncias on-demand, mas se não houver capacidade suficiente disponível, poderá usar algumas instâncias `c4.2xlarge` durante o pico de carga. Neste caso, a Frota do EC2 tenta atender a toda sua capacidade de destino usando instâncias `c5.2xlarge`, mas se não houver capacidade suficiente, ela executará automaticamente as instâncias `c4.2xlarge` para atender à capacidade de destino.

Priorizar tipos de instâncias para capacidade sob demanda

Quando Frota do EC2 tenta atender à sua capacidade sob demanda, o padrão é iniciar primeiro o tipo de instância de menor preço. Se `AllocationStrategy` estiver definido como `prioritized`, Frota do EC2 usará a prioridade para determinar qual tipo de instância será o primeiro para atender a capacidade sob demanda. A prioridade é atribuída à substituição do modelo de ativação, e a prioridade mais alta é lançada primeiro.

Por exemplo, você configurou três substituições de modelo de ativação, cada uma com um tipo de instância diferente: `c3.large`, `c4.large` e `c5.large`. O preço sob demanda para `c5.large` é menor do que para `c4.large`. `c3.large` é o mais barato. Se você não usar a prioridade para determinar o pedido, a frota atenderá à capacidade sob demanda começando com `c3.large` e, em seguida, `c5.large`. Como, muitas vezes, há Instâncias reservadas não usados para `c4.large`, você pode definir a prioridade de substituição do modelo de ativação para que a ordem seja `c4.large`, `c3.large` e `c5.large`.

Use Reservas de Capacidade para Instâncias on-demand

Com as Reservas de Capacidade sob demanda, você pode reservar capacidade computacional para suas Instâncias sob demanda em uma determinada zona de disponibilidade por qualquer duração. É possível configurar uma Frota do EC2 para usar as Reservas de Capacidade primeiro ao iniciar Instâncias sob demanda.

As Reservas de Capacidade são configuradas como `open` ou `targeted`. A frota EC2 pode iniciar Instâncias sob demanda nas Reservas de Capacidade `open` ou `targeted`, da seguinte forma:

- Se uma Reserva de capacidade é `open`, as Instâncias sob demanda que tiverem atributos correspondentes serão executadas automaticamente na capacidade reservada.
- Se uma Reserva de capacidade for `targeted`, as Instâncias sob demanda deverão usá-la como destino especificamente para executar na capacidade reservada. Isso é útil para usar Reservas de Capacidade específicas ou para controlar quando usar Reservas de Capacidade específicas.

Se você usar Reservas de Capacidade `targeted` em sua frota EC2, deve haver Reservas de Capacidade suficientes para atender à capacidade sob demanda de destino, caso contrário, o lançamento falhará. Para evitar uma falha no lançamento, adicione as Reservas de Capacidade `targeted` a um grupo de recursos e, em seguida, direcione o grupo de recursos. O grupo de recursos não precisa ter Reservas de Capacidade suficientes; se ficar sem Reservas de Capacidade antes que a capacidade sob demanda de

destino seja atendida, a frota poderá iniciar a capacidade de destino restante na capacidade sob demanda regular.

Para usar Reservas de Capacidade com a frota EC2

1. Configurar a frota como tipo `instant`. Não é possível usar Reservas de Capacidade para frotas de outros tipos.
2. Configure a estratégia de uso para Reservas de Capacidade como `use-capacity-reservations-first`.
3. No modelo de lançamento, para Reserva de capacidade, escolha Aberto ou Destino por grupo. Se escolher Destino por grupo, especifique o ID do grupo de recursos de Reservas de Capacidade.

Quando a frota tenta atender à capacidade sob demanda, se descobrir que vários grupos de instâncias têm Reservas de Capacidade correspondentes não utilizadas, ela determina os grupos nos quais iniciar as Instâncias sob demanda com base na estratégia de alocação sob demanda (`lowest-price` ou `prioritized`).

Para obter exemplos de como configurar uma frota para usar Reservas de Capacidade para atender à capacidade sob demanda, consulte [Exemplos de configuração de Frota do EC2 \(p. 824\)](#), especificamente os Exemplos 5 a 7.

Para obter informações sobre configuração das Reservas de Capacidade, consulte [On-Demand Capacity Reservations \(p. 390\)](#) e as [Perguntas frequentes sobre Reservas de Capacidade](#).

Rebalanceamento de capacidade

Você pode configurar a EC2 Fleet para iniciar uma instância spot de substituição quando o Amazon EC2 emitir uma recomendação de rebalanceamento para notificar que uma instância spot está em um risco elevado de interrupção. O rebalanceamento de capacidade ajuda a manter a disponibilidade da workload aumentando proativamente sua frota com uma nova instância spot antes que uma instância em execução seja interrompida por Amazon EC2. Para obter mais informações, consulte [Recomendações de rebalanceamento de instâncias do EC2 \(p. 333\)](#).

Para configurar a EC2 Fleet para executar uma instância spot de substituição, use o comando `create-fleet` (AWS CLI) e os parâmetros relevantes na estrutura de `MaintenanceStrategies`. Para obter mais informações, consulte o [exemplo de configuração de execução \(p. 834\)](#).

Limitações

- Disponível apenas para frotas do tipo `maintain`.
- Quando a frota estiver em execução, não é possível modificar a configuração de rebalanceamento de capacidade. Para alterar a configuração de rebalanceamento de capacidade, você deve excluir a frota e criar uma nova.

Considerações

Se você configurar uma Frota do EC2 para rebalanceamento de capacidade, considere o seguinte:

A Frota do EC2 pode executar a nova Instâncias spot de substituição até que a capacidade satisfeita seja a capacidade dobro de destino

Quando uma Frota do EC2 é configurada para rebalanceamento de capacidade, a frota tenta executar uma nova instância spot de substituição para cada instância spot que recebe uma recomendação de rebalanceamento. Depois que uma instância spot receber uma recomendação de rebalanceamento, ela não é mais contada como parte da capacidade de atendimento e a Frota do EC2 não encerra automaticamente a instância. Isso dá a você a oportunidade de executar [ações de rebalanceamento \(p. 334\)](#) na instância. Depois disso, você pode encerrar a instância ou deixá-la em execução.

Se sua frota atingir o dobro da capacidade de destino, ela interrompe a execução de novas instâncias de substituição, mesmo que as próprias instâncias de substituição recebam uma recomendação de rebalanceamento.

Por exemplo, você cria uma Frota do EC2 com uma capacidade de destino de 100 instâncias spot. Todas as instâncias spot recebem uma recomendação de rebalanceamento, o que faz com que a Frota do EC2 execute 100 instâncias spot substitutas. Isso eleva o número de instâncias spot atendidas para 200, o que é o dobro da capacidade de destino. Algumas das instâncias de substituição recebem uma recomendação de rebalanceamento, porém nenhuma instância de substituição é executada porque a frota não pode exceder o dobro da capacidade de destino.

Observe que você é cobrado por todas as instâncias durante a execução.

Recomendamos que você encerre manualmente as instâncias spot que recebem uma recomendação de rebalanceamento

Se você configurar a Frota do EC2 para rebalanceamento de capacidade, recomendamos que você monitore o sinal de recomendação de rebalanceamento recebido pelas instâncias spot na frota.

Ao monitorar o sinal, você pode executar rapidamente [ações de rebalanceamento \(p. 334\)](#) nas instâncias afetadas, antes que o Amazon EC2 as interrompa e, em seguida, você pode encerrá-las manualmente. Se você não encerrar as instâncias, continuará pagando por elas enquanto estiverem em execução. A EC2 Fleet não encerra automaticamente as instâncias que recebem uma recomendação de rebalanceamento.

Você pode configurar notificações usando o Amazon EventBridge ou metadados da instância. Para obter mais informações, consulte [Monitorar os sinais de recomendação de rebalanceamento \(p. 334\)](#).

A Frota do EC2 não conta as instâncias que recebem uma recomendação de rebalanceamento ao calcular a capacidade atendida durante o aumento ou a diminuição

Se a Frota do EC2 estiver configurada para rebalanceamento de capacidade e você alterar a capacidade de destino para aumento ou diminuição, a frota não contará as instâncias marcadas para rebalanceamento como parte da capacidade atendida, como a seguir:

- Diminuição – Se você diminuir a capacidade de destino desejada, a frota encerrará instâncias que não estão marcadas para rebalanceamento até que a capacidade desejada seja atingida. As instâncias marcadas para reequilíbrio não são contabilizadas para a capacidade atendida.

Por exemplo, você cria uma EC2 Fleet com uma capacidade planejada de 100 instâncias spot. 10 instâncias recebem uma recomendação de rebalanceamento, portanto, a frota inicia 10 novas instâncias de substituição, resultando em uma capacidade atendida de 110 instâncias. Em seguida, você reduz a capacidade de destino para 50 (diminuição), mas a capacidade de atendimento é, na verdade, 60 instâncias porque as 10 instâncias marcadas para rebalanceamento não são encerradas pela frota. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

- Aumento – Se você aumentar a capacidade desejada, a frota iniciará novas instâncias até que a capacidade desejada seja atingida. As instâncias marcadas para reequilíbrio não são contabilizadas para a capacidade atendida.

Por exemplo, você cria uma EC2 Fleet com uma capacidade planejada de 100 instâncias spot. 10 instâncias recebem uma recomendação de rebalanceamento, portanto, a frota inicia 10 novas instâncias de substituição, resultando em uma capacidade atendida de 110 instâncias. Em seguida, você aumenta a capacidade de destino para 200 (aumento), mas a capacidade de atendimento é, na verdade, 210 instâncias porque as 10 instâncias marcadas para rebalanceamento não são contabilizadas pela frota como parte da capacidade de destino. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

Forneça o maior número possível de grupos de capacidade spot na solicitação

Configure sua Frota do EC2 para usar vários tipos de instância e zonas de disponibilidade. Isso oferece a flexibilidade para executar instâncias spot em vários grupos de capacidade spot. Para obter mais informações, consulte [Ser flexível sobre tipos de instância e zonas de disponibilidade \(p. 303\)](#).

Configure sua Frota do EC2 para usar os grupos de capacidade spot mais adequados

Use a estratégia de alocação de `capacity-optimized` para garantir que as instâncias spot de substituição sejam executadas nos grupos de capacidade spot mais adequados. Para obter mais informações, consulte [Usar a estratégia de alocação otimizada por capacidade \(p. 304\)](#).

Sobreposições de preço máximo

Cada Frota do EC2 pode incluir um preço máximo global ou usar o padrão (preço sob demanda). A frota usa esse preço como o preço máximo padrão em cada uma das suas especificações de execução.

É possível especificar um preço máximo em uma ou mais especificações de execução. Esse preço é específico da especificação de execução. Se uma especificação de execução incluir um preço específico, a Frota do EC2 usará esse preço máximo para substituir o preço máximo global. Qualquer outra especificação de execução que não inclua um preço máximo específico ainda usará o preço máximo global.

Controle de gastos

O Frota do EC2 interrompe as instâncias de lançamento quando atingir um dos seguintes parâmetros: `TotalTargetCapacity` ou `MaxTotalPrice` (a quantidade máxima que você está disposto a pagar). Para controlar a quantidade paga por hora da sua frota, especifique `MaxTotalPrice`. Quando o preço total máximo for alcançado, o Frota do EC2 para de iniciar instâncias mesmo que não tenha atingido a capacidade alvo.

Os exemplos a seguir mostram duas situações diferentes. Na primeira, o Frota do EC2 para de executar instâncias ao atingir a capacidade de destino. Na segunda, o Frota do EC2 para de abrir instâncias ao atingir o valor máximo que você está disposto a pagar (`MaxTotalPrice`).

Exemplo: parar de executar instâncias quando a capacidade de destino for atingida

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 1,50 USD

O Frota do EC2 abre 10 Instâncias on-demand, porque o total de 1,00 USD (10 instâncias x 0,10 USD) não excede o `MaxTotalPrice` de 1,50 USD para Instâncias on-demand.

Exemplo: parar de executar instâncias quando o preço máximo total for atingido

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 0,80 USD

Se o Frota do EC2 executar a capacidade de destino (10 Instâncias on-demand), o custo total por hora será de 1,00 USD. Isso é mais que a quantidade (0,80 USD) especificada para `MaxTotalPrice` para Instâncias on-demand. Para evitar gastar mais do que você pretende, o Frota do EC2 abre somente 8 Instâncias on-demand (abaixo da capacidade de destino sob demanda), porque abrir mais excederia o `MaxTotalPrice` de Instâncias on-demand.

Peso de instâncias da Frota do EC2

Ao criar um Frota do EC2, você pode definir as unidades de capacidade com que cada tipo de instância contribuiria para a performance da aplicação. Você pode ajustar o preço máximo para cada especificação de lançamento usando peso de instâncias.

Por padrão, o preço que você especifica é por hora de instância. Ao usar o recurso de peso da instância, o preço que você especifica é por hora. Você pode calcular o preço por hora dividindo seu preço para um tipo de instância pelo número de unidades que ele representa. A EC2 Fleet calcula o número de instâncias a serem executadas dividindo a capacidade de destino pelo peso da instância. Se o resultado não for um valor inteiro, a frota o arredondará para o próximo valor inteiro, para que o tamanho de sua frota não fique abaixo de sua capacidade de destino. A frota pode selecionar qualquer grupo que você determinar na especificação de execução, mesmo que a capacidade das instâncias executadas ultrapasse a capacidade de destino solicitada.

A tabela a seguir inclui exemplos de cálculos para determinar o preço por unidade para uma Frota do EC2 com capacidade de destino igual a 10.

Tipo de instância	Peso da instância	Capacidade de destino	Número de instâncias executadas	Preço por hora de instância	Preço por hora
r3.xlarge	2	10	5 (10 dividido por 2)	0,05 USD	0,025 USD (0,05 dividido por 2)
r3.8xlarge	8	10	2 (10 dividido por 8, resultado arredondado para cima)	0,10 USD	0,0125 USD (0,10 dividido por 8)

Use o peso de instância da Frota do EC2 da maneira a seguir para provisionar a capacidade desejada de destino nos grupos com o menor preço por unidade no momento do atendimento:

1. Defina a capacidade de destino da Frota do EC2 em instâncias (o padrão) ou nas unidades de sua preferência, como CPUs virtuais, memória, armazenamento ou throughput.
2. Defina o preço por unidade.
3. Para cada especificação de execução, defina o peso, que é o número de unidades que o tipo de instância representa em relação à capacidade de destino.

Exemplo de peso da instância

Considere uma solicitação de Frota do EC2 com a seguinte configuração:

- Uma capacidade de destino de 24
- Uma especificação de execução com um tipo de instância r3.2xlarge e um peso de 6
- Uma especificação de execução com um tipo de instância c3.xlarge e um peso de 5

Os pesos representam o número de unidades que o tipo de instância representa em relação à capacidade de destino. Se a primeira especificação de execução fornecer o menor preço por unidade (preço de

`r3.2xlarge` por hora de instância dividido por 6), a Frota do EC2 executará quatro dessas instâncias (24 dividido por 6).

Se a segunda especificação de execução fornecer o menor preço por unidade (preço de `c3.xlarge` por hora de instância dividido por 5), a Frota do EC2 executará cinco dessas instâncias (24 dividido por 5, resultado arredondado para cima).

Peso da instância e estratégia de alocação

Considere uma solicitação de Frota do EC2 com a seguinte configuração:

- Uma capacidade de destino de 30 Instâncias spot
- Uma especificação de execução com um tipo de instância `c3.2xlarge` e um peso de 8
- Uma especificação de execução com um tipo de instância `m3.xlarge` e um peso de 8
- Uma especificação de execução com um tipo de instância `r3.xlarge` e um peso de 8

A Frota do EC2 executará quatro instâncias (30 dividido por 8, resultado arredondado para cima). Com a estratégia `lowest-price`, todas as quatro instâncias vêm do grupo que fornece o menor preço por unidade. Com a estratégia `diversified`, a frota executa uma instância em cada um dos três grupos, e a quarta instância em qualquer um dos três grupos fornece o menor preço spot por unidade.

Trabalhar com Frotas do EC2

Para usar uma Frota do EC2, crie uma solicitação que inclua a capacidade total de destino, a capacidade sob demanda, a capacidade spot, uma ou mais especificações de execução para as instâncias e o preço máximo que você está disposto a pagar. O solicitação de frota deve incluir um modelo de lançamento que defina as informações de que a frota precisa para executar um instância, como uma AMI, um tipo de instância, uma sub-rede ou uma zona de disponibilidade, e um ou mais security groups. É possível definir sobreposições de especificação de execução para o tipo de instância, a sub-rede, a zona de disponibilidade e o preço máximo que você está disposto a pagar, além de atribuir capacidade ponderada a cada sobreposição de especificação de execução.

Se a frota incluir a `Instâncias spot`, o Amazon EC2 poderá tentar manter a capacidade de destino da frota à medida que os preços spot são alterados.

Uma solicitação de tipo de Frota do EC2 `maintain` ou `request` permanecerá ativa até que expire ou você a exclua. Ao excluir uma frota do tipo `maintain` ou `request`, você poderá especificar se a exclusão encerrará ou não as instâncias dessa frota.

Tópicos

- [Estados das solicitações da Frota do EC2 \(p. 741\)](#)
- [Pré-requisitos da Frota do EC2 \(p. 743\)](#)
- [Verificações de integridade da Frota do EC2 \(p. 745\)](#)
- [Gerar um arquivo de configuração JSON da Frota do EC2 \(p. 746\)](#)
- [Criar uma Frota do EC2. \(p. 751\)](#)
- [Marcar uma Frota do EC2 \(p. 753\)](#)
- [Monitorar a Frota do EC2 \(p. 755\)](#)
- [Modificar uma Frota do EC2 \(p. 756\)](#)
- [Excluir uma Frota do EC2 \(p. 757\)](#)

Estados das solicitações da Frota do EC2

Uma solicitação de Frota do EC2 pode estar em um dos seguintes estados:

submitted

A solicitação de Frota do EC2 está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de destino de instâncias. A solicitação pode incluir Instâncias on-demand, Instâncias spot, ou ambos.

active

A solicitação de Frota do EC2 foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias em execução. A solicitação permanece nesse estado até que seja alterada ou excluída.

modifying

A solicitação de Frota do EC2 está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada ou que a solicitação seja excluída. Apenas um tipo `maintain` de frota pode ser modificado. Esse estado não se aplica a outros tipos de solicitação.

deleted_running

A solicitação de Frota do EC2 foi excluída e não executará instâncias adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas manualmente. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas. Apenas uma Frota do EC2 do tipo `maintain` ou `request` pode ter instâncias em execução após a solicitação de Frota do EC2 ser excluída. Uma frota `instant` excluída com instâncias em execução não é suportada. Este estado não se aplica às frotas `instant`.

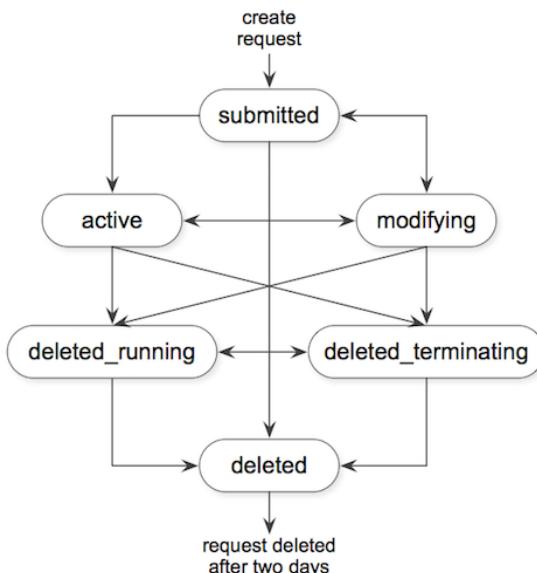
deleted_terminating

A solicitação de Frota do EC2 foi excluída, e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

deleted

A Frota do EC2 foi excluída, e não há outras instâncias em execução. A solicitação foi excluída dois dias depois que as instâncias foram encerradas.

A ilustração a seguir representa as transições entre os estados da solicitação de Frota do EC2. Se você exceder os limites da frota, a solicitação será excluída imediatamente.



Pré-requisitos da Frota do EC2

Para criar uma Frota do EC2, observe os seguintes pré-requisitos:

- [Modelo de execução \(p. 743\)](#)
- [Função vinculada ao serviço para Frota do EC2 \(p. 743\)](#)
- [Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS \(p. 744\)](#)
- [Permissões para usuários IAM da Frota do EC2 \(p. 744\)](#)

Modelo de execução

Um modelo de execução inclui informações sobre as instâncias a serem executadas, , por exemplo, o tipo de instância, a zona de disponibilidade e o preço máximo que você está disposto a pagar. Para obter mais informações, consulte [Executar uma instância a partir de um modelo de execução \(p. 425\)](#).

Função vinculada ao serviço para Frota do EC2

O `AWSServiceRoleForEC2Fleet` concede à EC2 Fleet permissão para solicitar, executar, encerrar e marcar instâncias em seu nome. O Amazon EC2 usa essa função vinculada ao serviço para concluir as seguintes ações:

- `ec2:RunInstances` – Executar instâncias
- `ec2:RequestSpotInstances` – Solicitação Instâncias spot.
- `ec2:TerminateInstances` – Encerrar instâncias
- `ec2:DescribeImages` – Descrever imagens de máquina da Amazon (AMIs) para Instâncias spot
- `ec2:DescribeInstanceStatus` – Descreva o status das Instâncias spot.
- `ec2:DescribeSubnets` – Descreva as sub-redes para Instâncias spot.
- `ec2>CreateTags` – Adicionar tags a Frota do EC2, instâncias e volumes.

Verifique se esta função está disponível antes de usar a AWS CLI ou uma API para criar uma EC2 Fleet.

Note

Uma Frota do EC2 instant não requer essa função.

Para criar a função, use o console do IAM da seguinte forma.

Para criar a função AWSServiceRoleForEC2Fleet para Frota do EC2

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Roles e Create role.
3. Em Select type of trusted entity (Selecionar tipo de entidade confiável), escolha AWS service (Produto da AWS).
4. Para Choose the service that will use this role (Escolher o serviço que usará essa função), selecione EC2 - Fleet (EC2 - Frota) e depois selecione Next: Permissions (Próximo: permissões), Next: Tags (Próximo: tags) e Next: Review (Próximo: análise).
5. Na página Review (Revisar), selecione Create role (Criar função).

Se você não precisar mais usar Frota do EC2, é recomendável excluir a função `AWSServiceRoleForEC2Fleet`. Depois que essa função for excluída na sua conta, você poderá criar a função novamente se criar outra frota.

Para obter mais informações, consulte [Usar funções vinculadas ao serviço](#) no Guia do usuário do IAM.

Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS

Se você especificar uma [AMI criptografada \(p. 135\)](#) ou um [snapshot do Amazon EBS criptografado \(p. 1422\)](#) na EC2 Fleet e usar uma chave do AWS KMS para criptografia, deverá conceder à função `AWSServiceRoleForEC2Fleet` permissão para usar a chave gerenciada pelo cliente de forma que o Amazon EC2 consiga executar instâncias em seu nome. Para isso, adicione uma concessão à chave gerenciada pelo cliente, conforme exibido no procedimento a seguir.

Durante a definição de permissões, as concessões são uma alternativa às políticas de chave. Para obter mais informações, consulte [Using grants \(Usar concessões\)](#) e [Using key policies in AWS KMS \(Usar políticas de chave no AWS KMS\)](#) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

Para conceder as permissões para a função `AWSServiceRoleForEC2Fleet` para usar a chave gerenciada pelo cliente

- Use o comando `create-grant` para adicionar uma concessão à chave gerenciada pelo cliente e especificar a entidade principal (a função vinculada ao serviço `AWSServiceRoleForEC2Fleet`) que recebe permissão para executar as operações permitidas pela concessão. A chave gerenciada pelo cliente é especificada pelo parâmetro `key-id` e o ARN da chave gerenciada pelo cliente. O principal é especificado pelo parâmetro `grantee-principal` e o ARN da função vinculada ao serviço `AWSServiceRoleForEC2Fleet`.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
    "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
    "ReEncryptTo"
```

Permissões para usuários IAM da Frota do EC2

Se os usuários do IAM vão criar ou gerenciar uma Frota do EC2, certifique-se de conceder a eles as permissões necessárias da maneira a seguir.

Para conceder aos usuários do IAM as permissões para a Frota do EC2

- Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
- No painel de navegação, selecione Policies (Políticas).
- Escolha Create policy (Criar política).
- Na página Create policy (Criar política), escolha a guia JSON, substitua texto pelo seguinte e escolha Review policy (Revisar política).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo"
            ],
            "Resource": "*"
        }
    ]
}
```

```
        "Effect": "Allow",
        "Action": [
            "iam>ListRoles",
            "iam>PassRole",
            "iam>ListInstanceProfiles"
        ],
        "Resource": "*"
    }
}
```

O `ec2:*` concede a um usuário do IAM permissão para chamar todas as ações de API do Amazon EC2. Para limitar o usuário a ações de API do Amazon EC2, especifique essas ações.

Um usuário do IAM deve ter permissão para chamar a ação `iam>ListRoles` para enumerar as funções do IAM existentes, a ação `iam>PassRole` para especificar a função da Frota do EC2 e a ação `iam>ListInstanceProfiles` para enumerar os perfis de instância existentes.

(Opcional) Para permitir que um usuário do IAM crie funções ou perfis de instância usando o console do IAM, você também deve adicionar as seguintes ações à política:

- `iam>AddRoleToInstanceProfile`
 - `iam>AttachRolePolicy`
 - `iam>CreateInstanceProfile`
 - `iam>CreateRole`
 - `iam>GetRole`
 - `iam>ListPolicies`
5. Na página Review policy (Revisar política), digite um nome e uma descrição para a política e escolha Create policy (Criar política).
 6. No painel de navegação, escolha Users (Usuários) e selecione o usuário.
 7. Na guia Permissions (Permissões), escolha Add permissions (Adicionar permissões).
 8. Selecione Attach existing policies directly. Selecione a política que você criou anteriormente e escolha Next: Review (Próximo: Revisão).
 9. Selecione Add permissions.

Verificações de integridade da Frota do EC2

A Frota do EC2 verifica o status de integridade das instâncias na frota a cada dois minutos. O status de integridade de uma instância é `healthy` ou `unhealthy`.

A Frota do EC2 determina o status de integridade de uma instância usando as verificações de status fornecidas pelo Amazon EC2. Uma instância é determinada como `unhealthy` quando o status da verificação de status da instância ou da verificação de status do sistema for `impaired` para três verificações de status de integridade consecutivas. Para obter mais informações, consulte [Verificações de status para as instâncias \(p. 867\)](#).

Você pode configurar a sua frota para substituir Instâncias spot não íntegras. Depois de configurar `ReplaceUnhealthyInstances` como `true`, uma instância spot é substituída ao ser reportada como `unhealthy`. A frota poderá ficar abaixo de sua capacidade de destino por alguns minutos enquanto uma instância spot não íntegra estiver sendo substituída.

Requirements

- A substituição da verificação de integridade é compatível apenas para Frotas do EC2 que mantenham uma capacidade de destino (frotas do tipo `maintain`) e não para as frotas únicas do tipo `request` ou `instant`.

- A substituição da verificação de integridade é compatível apenas para Instâncias spot. Este recurso não é compatível para Instâncias on-demand.
- Você pode configurar a Frota do EC2 para substituir instâncias não íntegras somente durante sua criação.
- Os usuários do IAM poderão usar a substituição de verificação de integridade somente se tiverem permissão para chamar a ação `ec2:DescribeInstanceStatus`.

Para configurar um Frota do EC2 para substituir uma Instâncias spot não íntegra

1. Siga as etapas para criar um Frota do EC2. Para obter mais informações, consulte [Criar uma Frota do EC2. \(p. 751\)](#).
2. Para configurar a frota para substituir Instâncias spot não íntegras no arquivo JSON para `ReplaceUnhealthyInstances`, insira `true`.

Gerar um arquivo de configuração JSON da Frota do EC2

Para criar uma Frota do EC2, basta especificar o modelo de execução, a capacidade total de destino e se a opção de compra padrão é sob demanda ou Spot. Se você não especificar esse parâmetro, a frota usará o valor padrão. Para visualizar a lista completa de parâmetros para configuração de frota, você pode gerar um arquivo JSON da seguinte forma.

Para gerar um arquivo JSON com todos os parâmetros de Frota do EC2 possíveis usando a linha de comando

- Use o comando `create-fleet` (AWS CLI) e o parâmetro `--generate-cli-skeleton` para gerar um arquivo JSON de EC2 Fleet:

```
aws ec2 create-fleet \
--generate-cli-skeleton
```

Os seguintes parâmetros de Frota do EC2 estão disponíveis:

```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "lowest-price",
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MaxTotalPrice": 0,
        "MinTargetCapacity": 0
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MaxTotalPrice": 0,
        "MinTargetCapacity": 0
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": ""
            }
        }
    ]
}
```

```
        "Version": "",  
    },  
    "Overrides": [  
        {  
            "InstanceType": "t2.micro",  
            "MaxPrice": "",  
            "SubnetId": "",  
            "AvailabilityZone": "",  
            "WeightedCapacity": null,  
            "Priority": null,  
            "Placement": {  
                "AvailabilityZone": "",  
                "Affinity": "",  
                "GroupName": "",  
                "PartitionNumber": 0,  
                "HostId": "",  
                "Tenancy": "dedicated",  
                "SpreadDomain": ""  
            }  
        }  
    ]  
},  
"TargetCapacitySpecification": {  
    "TotalTargetCapacity": 0,  
    "OnDemandTargetCapacity": 0,  
    "SpotTargetCapacity": 0,  
    "DefaultTargetCapacityType": "spot"  
},  
"TerminateInstancesWithExpiration": true,  
"Type": "maintain",  
"ValidFrom": "1970-01-01T00:00:00",  
"ValidUntil": "1970-01-01T00:00:00",  
"ReplaceUnhealthyInstances": true,  
"TagSpecifications": [  
    {  
        "ResourceType": "fleet",  
        "Tags": [  
            {  
                "Key": "",  
                "Value": ""  
            }  
        ]  
    }  
]
```

Referência do arquivo de configuração JSON da Frota do EC2

Note

Use letras minúsculas para todos os valores de parâmetros. Caso contrário, você receberá um erro quando o Amazon EC2 usar o arquivo JSON para executar a Frota do EC2.

AllocationStrategy (para SpotOptions)

(Opcional) Indica como alocar a capacidade prevista da instância spot em todos os grupos de capacidade spot especificados pela EC2 Fleet. Os valores válidos são `lowest-price`, `diversified`, `capacity-optimized`, `capacity-optimized-prioritized`. O padrão é `lowest-price`. Especifique a estratégia de alocação que atende às suas necessidades. Para obter mais informações, consulte [Estratégias de alocação para Instâncias spot \(p. 733\)](#).

InstanceInterruptionBehavior

(Opcional) O comportamento apresentado quando uma instância spot é interrompida. Os valores válidos são `hibernate`, `stop` e `terminate`. Por padrão, o serviço spot encerra Instâncias spot quando elas são interrompidas. Se o tipo de frota for `maintain`, você poderá especificar que o serviço spot coloque as Instâncias spot em hibernação ou as pare quando elas forem interrompidas.

InstancePoolsToUseCount

O número de grupos de capacidade spot para os quais alocar a capacidade spot prevista. Válido apenas quando a estratégia spot `AllocationStrategy` está definida como `lowest-price`. A EC2 Fleet seleciona os grupos de capacidade spot mais econômicos e aloca uniformemente sua capacidade spot de destino pelo número de grupos de capacidade spot que você especificar.

SingleInstanceType

Indica que a frota usa um único tipo de instância para abrir todos os Instâncias spot na frota.

SingleAvailabilityZone

Indica que a frota abre todos os Instâncias spot em uma única zona de disponibilidade.

MaxTotalPrice

O valor máximo por hora para o Instâncias spot que você está disposto a pagar.

MinTargetCapacity

A capacidade de destino mínima para o Instâncias spot na frota. Se a capacidade de destino mínima não for alcançada, a frota não abre nenhuma instância.

AllocationStrategy (para OnDemandOptions)

A ordem das substituições do modelo de execução para utilização de modo a atender a capacidade sob demanda. Se você especificar `lowest-price`, a Frota do EC2 usará o preço para determinar a ordem, executando o preço mais baixo primeiro. Se você especificar a prioridade, a Frota do EC2 usará a prioridade atribuída a cada substituição do modelo de ativação, executando a prioridade mais alta primeiro. Se você não especificar um valor, a Frota do EC2 definirá como padrão `lowest-price`.

SingleInstanceType

Indica que a frota usa um único tipo de instância para abrir todas as instâncias sob demanda da frota.

SingleAvailabilityZone

Indica que a frota abre todas as instâncias sob demanda em uma única zona de disponibilidade.

MaxTotalPrice

A quantidade máxima por hora para instâncias sob demanda que você está disposto a pagar.

MinTargetCapacity

A capacidade de destino mínima para instâncias sob demanda na frota. Se a capacidade de destino mínima não for alcançada, a frota não abre nenhuma instância.

ExcessCapacityTerminationPolicy

(Opcional) Indica se as instâncias em execução devem ser encerradas caso a capacidade total de destino da Frota do EC2 fique abaixo do tamanho atual da Frota do EC2. Os valores válidos são `no-termination` e `termination`.

LaunchTemplateId

O ID do modelo de execução a ser usado. Você deve especificar o ID do modelo de ativação ou o nome do modelo de execução. O modelo de execução deve especificar uma imagem de máquina da Amazon (AMI). Para obter mais informações sobre como criar modelos de execução, consulte [Executar uma instância a partir de um modelo de execução \(p. 425\)](#).

LaunchTemplateName

O nome do modelo de execução a ser usado. Você deve especificar o ID do modelo de ativação ou o nome do modelo de execução. O modelo de execução deve especificar uma imagem de máquina da Amazon (AMI). Para obter mais informações, consulte [Executar uma instância a partir de um modelo de execução \(p. 425\)](#).

Versão

O número da versão do modelo de execução, \$Latest ou \$Default. Você deve especificar um valor, caso contrário, a solicitação falhará. Se o valor for \$Latest, o Amazon EC2 usará a versão mais recente do modelo de execução. Se o valor for \$Default, o Amazon EC2 usará a versão padrão do modelo de execução. Para obter mais informações, consulte [Modificar um modelo de inicialização \(gerenciar versões do modelo de inicialização\) \(p. 434\)](#).

InstanceType

(Opcional) O tipo de instância. Se inserido, esse valor substitui o modelo de execução. Os tipos de instância devem ter as especificações mínimas necessárias de hardware (vCPUs, memória ou armazenamento).

MaxPrice

(Opcional) O preço máximo por hora que você está disposto a pagar por uma instância spot. Se inserido, esse valor substitui o modelo de execução. Você pode usar o preço máximo padrão (preço sob demanda) ou especificar o preço máximo que você está disposto a pagar. Suas Instâncias spot não serão executadas se seu preço máximo for inferior ao preço spot para os tipos de instâncias que você especificou.

SubnetId

(Opcional) O ID da sub-rede na qual as instâncias serão inicializadas. Se inserido, esse valor substitui o modelo de execução.

Para criar uma nova VPC, vá ao console do Amazon VPC. Quando você terminar, retorne ao arquivo JSON e insira o novo ID de sub-rede.

AvailabilityZone

(Opcional) A zona de disponibilidade na qual as instâncias são iniciadas. O padrão é permitir que a AWS escolha as zonas para suas instâncias. Se você preferir, pode selecionar zonas específicas. Se inserido, esse valor substitui o modelo de execução.

Especifique uma ou mais zonas de disponibilidade. Se você tiver mais de uma sub-rede em uma zona, especifique a sub-rede apropriada. Para adicionar sub-redes, acesse o console da Amazon VPC.

Quando você terminar, retorne ao arquivo JSON e insira o novo ID de sub-rede.

WeightedCapacity

(Opcional) O número de unidades fornecidas pelo tipo de instância especificado. Se inserido, esse valor substitui o modelo de execução.

Priority

A prioridade para a substituição do modelo de execução. A prioridade mais alta é executada primeiro.

Se a AllocationStrategy sob demanda estiver definida como prioritized, a EC2 Fleet usará a prioridade para determinar qual substituição de modelo de execução será usada primeiro para atender à capacidade sob demanda.

Se a AllocationStrategy spot estiver definida como capacity-optimized-prioritized, a EC2 Fleet usa a prioridade com base no melhor esforço para determinar qual modificação do modelo de lançamento usar primeiro para preencher a capacidade spot, mas otimiza a capacidade primeiro.

Os valores válidos são números inteiros começando em 0. Quanto menor o número, maior a prioridade. Se nenhum número for definido, a substituição do modelo de execução terá a menor

prioridade. Você pode definir a mesma prioridade para diferentes substituições de modelos de execução.

TotalTargetCapacity

O número de instâncias a serem executadas. Você pode escolher instâncias ou características de performance que são importantes para a workload de sua aplicação, como vCPUs, memória ou armazenamento. Se o tipo de solicitação for `maintain`, você poderá especificar uma capacidade de destino igual a 0 e adicionar capacidade posteriormente.

OnDemandTargetCapacity

(Opcional) O número de Instâncias on-demand a serem executadas. Esse número deve ser menor que `TotalTargetCapacity`.

SpotTargetCapacity

(Opcional) O número de Instâncias spot a serem executadas. Esse número deve ser menor que `TotalTargetCapacity`.

DefaultTargetCapacityType

Se o valor de `TotalTargetCapacity` for maior que os valores combinados de `OnDemandTargetCapacity` e `SpotTargetCapacity`, a diferença será executada como a opção de compra da instância especificada aqui. Os valores válidos são `on-demand` ou `spot`.

TerminateInstancesWithExpiration

(Opcional) Por padrão, o Amazon EC2 encerra suas instâncias quando a solicitação de Frota do EC2 expira. O valor padrão é `true`. Para manter as instâncias em execução após sua solicitação expirar, não insira um valor para esse parâmetro.

Tipo

(Opcional) O tipo de solicitação. Os valores válidos são `instant`, `request` e `maintain`. O valor padrão é `maintain`.

- `instant` – A Frota do EC2 envia uma solicitação única síncrona para a capacidade desejada e retorna erros para quaisquer instâncias que não puderam ser executadas.
- `request` – A Frota do EC2 envia uma solicitação única assíncrona para a capacidade desejada, mas envia solicitações spot em grupos de capacidade spot alternativos, se essa capacidade spot estiver indisponível e não mantém a capacidade spot se as Instâncias spot forem interrompidas.
- `maintain` – A Frota do EC2 envia uma solicitação assíncrona para a capacidade desejada e continua a manter a capacidade spot desejada, reabastecendo Instâncias spot interrompidas.

Para obter mais informações, consulte [Tipos de solicitação da Frota do EC2 \(p. 714\)](#).

ValidFrom

(Opcional) Para criar uma solicitação válida somente durante um período específico, insira uma data de início.

ValidUntil

(Opcional) Para criar uma solicitação válida somente durante um período específico, insira uma data de término.

ReplaceUnhealthyInstances

(Opcional) Para substituir instâncias não íntegras em uma Frota do EC2 configurada para `maintain` a frota, insira `true`. Caso contrário, deixe este parâmetro vazio.

TagSpecifications

(Opcional) Os pares de valor-chave para marcar a solicitação de Frota do EC2 na criação. O valor para `ResourceType` deve ser `fleet`, caso contrário, ocorrerá falha na solicitação de frota. Para

marcar instâncias na inicialização, especifique as tags no [modelo de execução \(p. 427\)](#). Para obter informações sobre marcação após a execução, consulte [Marcar com tag os recursos do \(p. 1555\)](#).

Criar uma Frota do EC2.

Ao criar uma Frota do EC2, você precisa especificar um modelo de execução que inclua informações sobre as instâncias a serem executadas, , por exemplo, o tipo de instância, a zona de disponibilidade e o preço máximo que você está disposto a pagar.

Você pode criar uma Frota do EC2 que inclua várias especificações de execução para substituir o modelo de execução. As especificações de execução podem variar por tipo de instância, zona de disponibilidade, sub-rede e preço máximo e podem incluir uma capacidade ponderada diferente.

Quando você cria um Frota do EC2, use um arquivo JSON para especificar informações sobre as instâncias a serem executadas. Para obter mais informações, consulte [Referência do arquivo de configuração JSON da Frota do EC2 \(p. 747\)](#).

As frotas do EC2 podem ser criadas somente com o uso da AWS CLI.

Criar uma EC2 Fleet (AWS CLI)

- Use o comando [create-fleet \(AWS CLI\)](#) para criar uma EC2 Fleet.

```
aws ec2 create-fleet \
--cli-input-json file:///file_name.json
```

Para obter arquivos de configuração de exemplo, consulte [Exemplos de configuração de Frota do EC2 \(p. 824\)](#).

A seguir está um exemplo de saída de uma frota do tipo `request` ou `maintain`.

```
{  
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"  
}
```

A seguir está um exemplo de saída de uma frota do tipo `instant` que executou a capacidade de destino.

```
{  
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",  
    "Errors": [],  
    "Instances": [  
        {  
            "LaunchTemplateAndOverrides": {  
                "LaunchTemplateSpecification": {  
                    "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",  
                    "Version": "1"  
                },  
                "Overrides": {  
                    "InstanceType": "c5.large",  
                    "AvailabilityZone": "us-east-1a"  
                }  
            },  
            "Lifecycle": "on-demand",  
            "InstanceIds": [  
                "i-1234567890abcdef0",  
                "i-9876543210abcdef9"  
            ],  
            "InstanceType": "c5.large",  
            "Status": "active",  
            "Type": "instant"  
        }  
    ]  
}
```

```
        "Platform": null
    },
{
    "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
            "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
            "Version": "1"
        },
        "Overrides": {
            "InstanceType": "c4.large",
            "AvailabilityZone": "us-east-1a"
        }
    },
    "Lifecycle": "on-demand",
    "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
    ],
    "InstanceType": "c4.large",
    "Platform": null
},
]
}
```

A seguir está um exemplo de saída de uma frota do tipo instant que executou parte da capacidade de destino com erros em instâncias que não foram executadas.

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
    "Errors": [
        {
            "LaunchTemplateAndOverrides": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
                    "Version": "1"
                },
                "Overrides": {
                    "InstanceType": "c4.xlarge",
                    "AvailabilityZone": "us-east-1a",
                }
            },
            "Lifecycle": "on-demand",
            "ErrorCode": "InsufficientInstanceCapacity",
            "ErrorMessage": "",
            "InstanceType": "c4.xlarge",
            "Platform": null
        },
    ],
    "Instances": [
        {
            "LaunchTemplateAndOverrides": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
                    "Version": "1"
                },
                "Overrides": {
                    "InstanceType": "c5.large",
                    "AvailabilityZone": "us-east-1a"
                }
            },
            "Lifecycle": "on-demand",
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-9876543210abcdef9"
            ]
        }
    ]
}
```

```
],
  "InstanceType": "c5.large",
  "Platform": null
},
]
}
```

A seguir está um exemplo de saída de uma frota do tipo instant que não executou nenhuma instância.

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": "",
      "InstanceType": "c4.xlarge",
      "Platform": null
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": "",
      "InstanceType": "c5.large",
      "Platform": null
    }
  ],
  "Instances": []
}
```

Marcar uma Frota do EC2

Para categorizar e gerenciar as solicitações de Frota do EC2, você pode marcá-las com metadados personalizados. Você pode atribuir uma tag a uma solicitação de Frota do EC2 ao criá-la ou posteriormente.

Quando você marca uma solicitação de frota, as instâncias e os volumes que são executados pela frota não são marcados automaticamente. É necessário marcar explicitamente as instâncias e os volumes executados pela frota. Você pode optar por atribuir tags somente à solicitação de frota, somente às instâncias executadas pela frota, somente aos volumes anexados às instâncias executadas pela frota ou aos todos os três.

Note

Para tipos de frota `instant`, é possível marcar volumes anexados a Instâncias on-demand e Instâncias spot. Para os tipos de frota `request` ou `maintain`, só é possível marcar volumes anexados a Instâncias on-demand.

Para obter mais informações sobre como as tags funcionam, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

Pré-requisito

Conceda ao usuário do IAM permissão para marcar recursos. Para obter mais informações, consulte [Exemplo: marcar recursos \(p. 1178\)](#).

Como conceder a um usuário do IAM permissão para marcar recursos

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:CreateTags`. Concede ao usuário do IAM permissão para criar tags.
- A ação `ec2:CreateFleet`. Concede ao usuário do IAM permissão para criar uma solicitação de Frota do EC2.
- Para `Resource`, recomendamos que você especifique `"*"`. Permite que os usuários marquem todos os tipos de recursos.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "TagEC2FleetRequest",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags",  
                "ec2:CreateFleet"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Important

No momento, não oferecemos suporte para permissões no nível do recurso para o recurso `create-fleet`. Se especificar `create-fleet` como um recurso, você receberá uma exceção não autorizada quando tentar marcar a frota. O exemplo a seguir ilustra como não definir a política.

```
{  
    "Effect": "Allow",  
    "Action": [  
        "ec2:CreateTags",  
        "ec2:CreateFleet"  
    ],  
    "Resource": "arn:aws:ec2:us-east-1:111122223333:create-fleet/*"  
}
```

Como marcar uma nova solicitação de Frota do EC2

Para marcar uma solicitação de Frota do EC2 ao criá-la, especifique o par de valor-chave no [arquivo JSON \(p. 746\)](#) usado para criar a frota. O valor de `ResourceType` deve ser `fleet`. Se você especificar outro valor, ocorrerá falha na frota.

Como marcar instâncias e volumes executado por uma Frota do EC2

Para marcar instâncias e volumes ao serem executados pela frota, especifique as tags no [modelo de execução \(p. 427\)](#) mencionado na solicitação de Frota do EC2.

Note

Não é possível marcar volumes anexados a Instâncias spot que são executados por um tipo de frota `request` ou `maintain`.

Para marcar uma solicitação de EC2 Fleet, uma instância e um volume existentes (AWS CLI)

Use o comando [create-tags](#) para marcar os recursos existentes.

```
aws ec2 create-tags \
  --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
  --tags Key=purpose,Value=test
```

Monitorar a Frota do EC2

A Frota do EC2 executa Instâncias on-demand quando há capacidade disponível e executa Instâncias spot quando o preço máximo excede o preço spot e há capacidade disponível. As Instâncias on-demand são executadas até que você as encerre, e as Instâncias spot são executadas até que sejam interrompidas ou encerradas.

A lista retornada das instâncias em execução é atualizada periodicamente e pode estar desatualizada.

Para monitorar a EC2 Fleet (AWS CLI)

Use o comando [describe-fleets](#) para descrever suas Frotas do EC2.

```
aws ec2 describe-fleets
```

A seguir está um exemplo de saída.

```
{
  "Fleets": [
    {
      "Type": "maintain",
      "FulfilledCapacity": 2.0,
      "LaunchTemplateConfigs": [
        {
          "LaunchTemplateSpecification": {
            "Version": "2",
            "LaunchTemplateId": "lt-07b3bc7625cdab851"
          }
        }
      ],
      "TerminateInstancesWithExpiration": false,
      "TargetCapacitySpecification": {
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 2,
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
      },
      "FulfilledOnDemandCapacity": 0.0,
      "ActivityStatus": "fulfilled",
      "FleetId": "fleet-76e13e99-01ef-4bd6-ba9b-9208de883e7f",
      "ReplaceUnhealthyInstances": false,
      "SpotOptions": {
```

```
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "AllocationStrategy": "lowest-price"
    },
    "FleetState": "active",
    "ExcessCapacityTerminationPolicy": "termination",
    "CreateTime": "2018-04-10T16:46:03.000Z"
}
]
```

Use o comando [describe-fleet-instances](#) para descrever as instâncias da Frota do EC2 especificada.

```
aws ec2 describe-fleet-instances \
--fleet-id fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE
```

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Use o comando [describe-fleet-history](#) para descrever o histórico da Frota do EC2 especificada na hora determinada.

```
aws ec2 describe-fleet-history --fleet-request-id fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE --start-time 2018-04-10T00:00:00Z
```

```
{
    "HistoryRecords": [],
    "FleetId": "fleet-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2018-04-09T23:53:20.000Z"
}
```

Modificar uma Frota do EC2

Você pode modificar uma Frota do EC2 no estado `submitted` ou `active`. Quando você modifica uma frota, ela entra no estado `modifying`.

Só é possível modificar uma Frota do EC2 do tipo `maintain`. Você não pode modificar uma Frota do EC2 do tipo `request` nem do tipo `instant`.

Você pode modificar os seguintes parâmetros de uma Frota do EC2:

- `target-capacity-specification` – Aumentar ou diminuir a capacidade de destino de `TotalTargetCapacity`, `OnDemandTargetCapacity` e `SpotTargetCapacity`.

- **excess-capacity-termination-policy** – Se as instâncias em execução devem ser encerradas caso a capacidade total de destino da Frota do EC2 fique abaixo do tamanho atual da frota. Os valores válidos são `no-termination` e `termination`.

Quando você aumenta a capacidade de destino, a Frota do EC2 executa as instâncias adicionais de acordo com a opção de compra da instância especificada para `DefaultTargetCapacityType`, ou seja, Instâncias on-demand ou Instâncias spot.

Se `DefaultTargetCapacityType` for `spot`, a Frota do EC2 executará as Instâncias spot adicionais de acordo com sua respectiva estratégia de alocação. Se a estratégia de alocação for `lowest-price`, a frota executará as instâncias do grupo de capacidade spot que apresentar o menor preço na solicitação. Se a estratégia de alocação for `diversified`, a frota distribuirá as instâncias pelos grupos na solicitação.

Quando você diminui a capacidade de destino, a Frota do EC2 excluirá todas as solicitações abertas que excedem a nova capacidade de destino. Você pode solicitar que a frota encerre instâncias até o tamanho da frota atingir a nova capacidade de destino. Se a estratégia de alocação for `lowest-price`, a frota encerrará as instâncias com o preço mais alto por unidade. Se a estratégia de alocação for `diversified`, a frota encerrará as instâncias nos grupos. Como alternativa, você pode solicitar que a Frota do EC2 mantenha seu tamanho atual, mas não substitua as Instâncias spot interrompidas ou encerradas manualmente.

Quando uma EC2 Fleet encerra uma instância spot porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

Para modificar uma EC2 Fleet (AWS CLI)

Use o comando `modify-fleet` para atualizar a capacidade de destino da Frota do EC2 especificada.

```
aws ec2 modify-fleet \
--fleet-id fleet-73fdbd2ce-aa30-494c-8788-1cee4EXAMPLE \
--target-capacity-specification TotalTargetCapacity=20
```

Se estiver diminuindo a capacidade de destino, mas quiser manter a frota com o tamanho atual, você poderá modificar o comando anterior da maneira a seguir.

```
aws ec2 modify-fleet \
--fleet-id fleet-73fdbd2ce-aa30-494c-8788-1cee4EXAMPLE \
--target-capacity-specification TotalTargetCapacity=10 \
--excess-capacity-termination-policy no-termination
```

Excluir uma Frota do EC2

Caso não precise mais de uma Frota do EC2, você pode excluí-la. Depois de excluir uma frota, ela não executará novas instâncias.

Ao excluir uma Frota do EC2, você deve especificar se deseja encerrar também suas instâncias. Se você especificar que as instâncias precisam ser encerradas quando a frota for excluída, ela entrará no estado `deleted_terminating`. Caso contrário, ela entrará no estado `deleted_running` e as instâncias continuarão em execução até que sejam interrompidas ou encerradas manualmente.

Restrictions

- Você pode excluir até 25 frotas instant de uma única solicitação. Se você exceder esse número, nenhuma frota instant será excluída e um erro será retornado. Não há restrição sobre o número de frotas do tipo `maintain` ou `request` que podem ser excluídas em uma única solicitação.
- Até 1000 instâncias podem ser encerradas em uma única solicitação para excluir frotas instant.

Para excluir uma EC2 Fleet e encerrar suas instâncias (AWS CLI)

Use o comando [delete-fleets](#) e o parâmetro --terminate-instances para excluir a Frota do EC2 especificada e encerrar as instâncias:

```
aws ec2 delete-fleets \
--fleet-ids fleet-73fb2ce-aa30-494c-8788-1cee4EXAMPLE \
--terminate-instances
```

A seguir está um exemplo de saída.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fb2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

Para excluir uma EC2 Fleet sem encerrar as instâncias (AWS CLI)

Você pode modificar o comando anterior usando o parâmetro --no-terminate-instances para excluir a Frota do EC2 especificada sem encerrar as instâncias.

Note

--no-terminate-instances não é suportado para frotas instant.

```
aws ec2 delete-fleets \
--fleet-ids fleet-73fb2ce-aa30-494c-8788-1cee4EXAMPLE \
--no-terminate-instances
```

A seguir está um exemplo de saída.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafaf4c6b7dcEXAMPLE"
        }
    ]
}
```

Solucionar problemas quando houver falha na exclusão da frota

Em caso de falha na exclusão da Frota do EC2, `UnsuccessfulFleetDeletions` retornará o ID da Frota do EC2, um código de erro e uma mensagem de erro.

Os códigos de erro são:

- `ExceededInstantFleetNumForDeletion`
- `fleetIdDoesNotExist`
- `fleetIdMalformed`

- fleetNotInDeletableState
- NoTerminateInstancesNotSupported
- UnauthorizedOperation
- unexpectedError

Solução de problemas do **ExceededInstantFleetNumForDeletion**

Se você tentar excluir mais de 25 frotas instant em uma única solicitação, o erro ExceededInstantFleetNumForDeletion será retornado. Veja a seguir um exemplo de saída deste erro.

```
{  
    "UnsuccessfulFleetDeletions": [  
        {  
            "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",  
            "Error": {  
                "Message": "Can't delete more than 25 instant fleets in a single  
request.",  
                "Code": "ExceededInstantFleetNumForDeletion"  
            }  
        },  
        {  
            "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",  
            "Error": {  
                "Message": "Can't delete more than 25 instant fleets in a single  
request.",  
                "Code": "ExceededInstantFleetNumForDeletion"  
            }  
        },  
        .  
        .  
        .  
    ],  
    "SuccessfulFleetDeletions": []  
}
```

Solução de problemas do **NoTerminateInstancesNotSupported**

Se você especificar que as instâncias em uma frota instant não devem ser encerradas quando você excluir a frota, o erro NoTerminateInstancesNotSupported será retornado. --no-terminate-instances não é suportado para frotas instant. Veja a seguir um exemplo de saída deste erro.

```
{  
    "UnsuccessfulFleetDeletions": [  
        {  
            "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",  
            "Error": {  

```

Solução de problemas do **UnauthorizedOperation**

Se você não tiver permissão para encerrar instâncias, você obterá o erro UnauthorizedOperation ao excluir uma frota que deve encerrar suas instâncias. A seguir está a resposta de erro.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not authorized to perform this operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-YjByeAU66Q9752NtQ-I3-qnDLWs6JLFdKnSMMiq5s6cGqjjPtEDpsnGHzyHasFHOaRYJpaDVravow25azn6KNkUQqlFwhJyujt2dtNCdduJfrqcFYAjleEiRMkfDht7N63SKlwBHTurzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVhbY9JhLvGypLcMuJtJ76H9ytg2zRVPiU5v2s-UgZ7h0p2yth6ysUdh1ONG6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-EMhekLFZeJLrDtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXXWVywzgnLtHeRf2o4lUhGBw17mXss07k7XAfdpPMPT9vrHtQiILor5VVTsjSPWg7edj_1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC9YPGMLK9</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</RequestID></Response>
```

Para resolver o erro, você deve adicionar a ação `ec2:TerminateInstances` à política do IAM, conforme mostrado no exemplo a seguir.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeleteFleetsAndTerminateInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteFleets",
                "ec2:TerminateInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Frota spot

Uma frota spot é um conjunto de instâncias spot e instâncias sob demanda opcionalmente executadas com base nos critérios especificados por você. A frota spot seleciona os grupos de capacidade spot que atendem às suas necessidades e executa instâncias spot para atender à capacidade prevista para a frota. Por padrão, as Frotas spot são definidas para manter a capacidade de destino executando instâncias de substituição depois que as Instâncias spot da frota são encerradas. Você pode enviar uma frota spot como uma solicitação única, que não persiste depois que as instâncias são encerradas. Você pode incluir solicitações de instância sob demanda em uma solicitação de frota spot.

Tópicos

- [Tipos de solicitação da frota spot \(p. 761\)](#)
- [Estratégias de configuração de frota spot \(p. 761\)](#)
- [Trabalhar com frotas spot \(p. 769\)](#)
- [Métricas do CloudWatch para frota spot \(p. 790\)](#)
- [Escalabilidade automática para frota spot \(p. 792\)](#)

Tipos de solicitação da frota spot

Há dois tipos de solicitações de frota spot:

`request`

Se você configurar o tipo de solicitação como `request`, a frota spot faz uma solicitação assíncrona única da capacidade desejada. Portanto, se a capacidade for reduzida devido a interrupções do spot, a frota não tentará reabastecer as Instâncias spot nem enviará solicitações em grupos de capacidade spot alternativos, se a capacidade não estiver disponível.

`maintain`

Se você configurar o tipo de solicitação como `maintain`, a frota spot faz uma solicitação assíncrona única da capacidade desejada e mantém a capacidade reabastecendo automaticamente quaisquer Instâncias spot interrompidas.

Para especificar o tipo de solicitação no console do Amazon EC2, faça o seguinte ao criar uma solicitação de frota spot:

- Para criar uma frota spot do tipo `request`, desmarque a caixa de seleção Manter a capacidade pretendida.
- Para criar uma frota spot do tipo `maintain`, marque a caixa de seleção Manter a capacidade pretendida.

Para obter mais informações, consulte [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 777\)](#).

Os dois tipos de solicitações se beneficiam com a estratégia de alocação. Para obter mais informações, consulte [Estratégia de alocação para Instâncias spot \(p. 762\)](#).

Estratégias de configuração de frota spot

A frota spot é uma coleção, ou frota, de instâncias spot e, opcionalmente, instâncias sob demanda.

A frota spot tenta executar o número de instâncias spot e instâncias sob demanda para atender à capacidade desejada especificada na solicitação de frota spot. A solicitação de Instâncias spot será

atendida se houver capacidade disponível e se o preço máximo especificado na solicitação exceder o preço spot atual. A frota spot também tenta manter sua frota de capacidade pretendida se as instâncias spot forem interrompidas.

Você também poderá definir um valor máximo por hora que esteja disposto a pagar pela frota, e a frota spot executará instâncias até alcançar o valor máximo. Quando o valor máximo que você está disposto a pagar for alcançado, a frota interromperá a execução de instâncias mesmo que a capacidade de destino ainda não tenha sido alcançada.

Um Grupo de capacidade Spot é um conjunto de instâncias do EC2 não usadas com o mesmo tipo de instância (por exemplo `m5.large`), sistema operacional, zona de disponibilidade e plataforma de rede. Ao criar uma solicitação de frota spot, você poderá incluir várias especificações de execução, que variam de acordo com o tipo de instância, a AMI, a zona de disponibilidade ou a sub-rede. A frota spot seleciona os grupos de capacidade spot que são usados para atender à solicitação com base nas especificações de execução incluídas na sua solicitação de frota spot e na configuração da solicitação de frota spot. As Instâncias spot vêm dos grupos selecionados.

Tópicos

- [Planejar uma solicitação de frota spot \(p. 762\)](#)
- [Estratégia de alocação para Instâncias spot \(p. 762\)](#)
- [Sob demanda na frota spot \(p. 765\)](#)
- [Rebalanceamento de capacidade \(p. 765\)](#)
- [Substituições do preço spot \(p. 767\)](#)
- [Controle de gastos \(p. 767\)](#)
- [Peso de instâncias de frotas spot \(p. 768\)](#)

Planejar uma solicitação de frota spot

Antes de criar uma solicitação de frota spot, leia as [Práticas recomendadas de spot](#). Use essas melhores práticas ao planejar a solicitação de frota spot para que você possa provisionar o tipo de instância desejado com o menor preço possível. Também recomendamos fazer o seguinte:

- Determine se você deseja criar uma frota spot que envie uma solicitação única para a capacidade de destino desejada ou uma frota spot que mantenha uma capacidade de destino ao longo do tempo.
- Determine os tipos de instâncias que atendem aos requisitos do aplicativo.
- Determine a capacidade de destino da solicitação de frota spot. Você pode definir a capacidade de destino em instâncias ou em unidades personalizadas. Para obter mais informações, consulte [Peso de instâncias de frotas spot \(p. 768\)](#).
- Determine a parte da capacidade de destino da frota spot que deve ser sob demanda. Você pode especificar 0 para a capacidade sob demanda.
- Determine seu preço por unidade, se você estiver usando o peso de instância. Para calcular o preço por unidade, divida o preço por hora de instância pelo número de unidades (ou peso) que essa instância representa. Se você não estiver usando o peso de instância, o preço padrão por unidade será o preço por hora de instância.
- Leia as opções possíveis para a solicitação de frota spot. Para obter mais informações, consulte o comando `request-spot-fleet` na AWS CLI Command Reference (Referência de comandos da AWS CLI). Para obter exemplos adicionais, consulte [Exemplos de configuração de frota spot \(p. 837\)](#).

Estratégia de alocação para Instâncias spot

A estratégia de alocação para instâncias spot em sua frota spot determina como ela atenderá à solicitação de frota spot dos possíveis grupos de capacidade spot representados por suas especificações de execução. Veja a seguir as estratégias de alocação que você pode especificar na solicitação de frota spot:

`lowestPrice`

As Instâncias spot vêm do grupo com o menor preço. Essa é a estratégia padrão.
`diversified`

As Instâncias spot são distribuídas por todos os grupos.

`capacityOptimized`

O Instâncias spot provém dos grupos com capacidade ideal para o número de instâncias em execução. Opcionalmente, você pode definir uma prioridade para cada tipo de instância na frota usando o `capacityOptimizedPrioritized`. A frota spot otimiza a capacidade primeiro, mas empenha-se em honrar as prioridades de tipo de instância.

Com as Instâncias spot, a definição de preço muda lentamente ao longo do tempo com base em tendências de longo prazo na oferta e na demanda, mas a capacidade oscila em tempo real. A estratégia `capacityOptimized` executa Instâncias spot automaticamente nos grupos mais disponíveis observando dados de capacidade em tempo real e prevendo quais os mais disponíveis. Isso funciona bem para workloads, como big data e análise, renderização de imagens e mídia, machine learning e computação de alta performance, que podem ter um custo de interrupção maior associado ao reinício do trabalho e ao ponto de verificação. Ao oferecer a possibilidade de menos interrupções, a estratégia `capacityOptimized` pode reduzir o custo geral da workload.

Como alternativa, você pode usar a estratégia de alocação `capacityOptimizedPrioritized` com um parâmetro de prioridade para ordenar os tipos de instância, da prioridade mais alta para a mais baixa. Você pode definir a mesma prioridade para diferentes tipos de instância. A frota spot otimizará a capacidade primeiro, mas se empenhará em honrar as prioridades de tipo de instância (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da frota spot de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante. Só haverá suporte para o uso de prioridades se a frota usar um modelo de lançamento. Observe que quando você define a prioridade para `capacityOptimizedPrioritized`, a mesma prioridade também será aplicada às instâncias sob demanda se o `AllocationStrategy` sob demanda estiver definido como `prioritized`.

`InstancePoolsToUseCount`

As Instâncias spot são distribuídas pelo número de grupos spot que você especifica. Este parâmetro é válido somente quando usado em combinação com `lowestPrice`.

Manter a capacidade de destino

Depois que as Instâncias spot são encerradas devido a uma alteração no preço spot ou na capacidade disponível de um grupo de capacidade spot, uma frota spot do tipo `maintain` executa as instâncias spot de substituição. Se a estratégia de alocação for `lowestPrice`, a frota executará instâncias de substituição no grupo onde o preço spot for atualmente o menor. Se a estratégia de alocação for `diversified`, a frota distribuirá as Instâncias spot de substituição pelos grupos restantes. Se a estratégia de alocação for `lowestPrice` em combinação com `InstancePoolsToUseCount`, a frota selecionará os grupos spot com o menor preço e lançará as Instâncias spot pelo número de grupos spot que você especificar.

Escolher uma estratégia de alocação apropriada

Você pode otimizar as Frotas spot com base em seu caso de uso.

Se a sua frota executar workloads que possam ter um custo maior de interrupção associado ao reinício de trabalho e ao ponto de verificação, use a estratégia `capacityOptimized`. Essa estratégia oferece a possibilidade de menos interrupções, o que pode reduzir o custo geral da workload. Essa é a estratégia recomendada. Use a estratégia `capacityOptimizedPrioritized` para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante.

Se a frota for pequena ou for executada por um período curto, a probabilidade de que as Instâncias spot possam ser interrompidas será baixa, mesmo com todas as instâncias em um único grupo de capacidade spot. Portanto, é provável que a estratégia `lowestPrice` atenda às suas necessidades enquanto oferece o menor custo.

Se sua frota é grande ou executa há muito tempo, você pode aprimorar a disponibilidade de sua frota distribuindo as Instâncias spot por vários grupos. Por exemplo, se a solicitação de frota spot especificar 10 grupos e uma capacidade pretendida de 100 instâncias, a frota executará 10 Instâncias spot em cada grupo. Se o preço spot para um grupo exceder seu preço máximo para esse mesmo grupo, somente 10% de sua frota será afetada. Usar essa estratégia também torna sua frota menos sensível a aumentos que ocorram com o tempo no preço spot em qualquer grupo específico. Com a estratégia `diversified`, a frota spot não executará instâncias spot em nenhum grupo com um preço spot igual ou maior que o [preço sob demanda](#).

Para criar uma frota econômica e diversificada, use a estratégia `lowestPrice` em combinação com `InstancePoolsToUseCount`. Você pode usar um número baixo ou alto de grupos spot para alocar suas Instâncias spot. Por exemplo, se você executar o processamento em lote, recomendamos que especifique um número baixo de grupos spot (por exemplo, `InstancePoolsToUseCount=2`) para garantir que sua fila sempre tenha capacidade computacional enquanto maximiza a economia. Se você executa um serviço Web, recomendamos que especifique um grande número de grupos Spot (por exemplo, `InstancePoolsToUseCount=10`) para minimizar o impacto, caso um grupo de capacidade Spot fique temporariamente indisponível.

Configurar a frota spot para otimização de custos

Para otimizar os custos de uso de Instâncias spot, especifique a estratégia de alocação `lowestPrice` de modo que a frota spot implante a combinação mais econômica de tipos de instância e zonas de disponibilidade de maneira automática e com base no preço spot atual.

Para a capacidade de destino de instância sob demanda, a frota spot sempre seleciona o tipo de instância mais econômico com base no preço público sob demanda e continua seguindo a estratégia de alocação (`lowestPrice`, `capacityOptimized` ou `diversified`) para Instâncias spot.

Configurar a frota spot para otimização de custos e diversificação

Para criar uma frota de instâncias spot econômica e diversificada, use a estratégia de alocação `lowestPrice` em combinação com `InstancePoolsToUseCount`. A frota spot implanta a combinação mais econômica de tipos de instância e zonas de disponibilidade de maneira automática e com base no preço spot atual no número de grupos spot especificado. Esta combinação pode ser usada para evitar as Instâncias spot mais caras.

Por exemplo, se a capacidade de destino for 10 Instâncias Spot e você especificar 2 pools de capacidade spot (para `InstancePoolsToUseCount`), a Spot Fleet utilizará os dois pools mais baratos para satisfazer a sua capacidade spot.

Observe que o Spot Fleet tenta extrair Instâncias Spot a partir do número de pools que você especificar com base no melhor esforço. Se um pool ficar sem capacidade spot antes de cumprir sua capacidade alvo, a Spot Fleet continuará atendendo à sua solicitação usando o próximo pool mais barato. Para garantir que sua capacidade de destino seja atendida, você pode receber Instâncias Spot de mais do que o número de pools especificado. Da mesma forma, se a maioria dos pools não tiver capacidade spot, você poderá receber sua capacidade de destino total de menos do que o número de pools que você especificou.

Configurar a frota spot para otimização de capacidade

Para iniciar instâncias spot nos grupos de capacidade spot mais disponíveis, use a estratégia de alocação `capacityOptimized`. Para obter uma configuração de exemplo, consulte [Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade \(p. 847\)](#).

Também é possível expressar as prioridades de seu grupo usando a estratégia de alocação `capacityOptimizedPrioritized` e definir a ordem dos tipos de instância a serem usados, da prioridade mais alta para a mais baixa. Só haverá suporte para o uso de prioridades se a frota usar um modelo de lançamento. Observe que, ao definir as prioridades para `capacityOptimizedPrioritized`, as mesmas prioridades também serão aplicadas às instâncias sob demanda se `OnDemandAllocationStrategy` estiver definido como `prioritized`. Para obter uma configuração de exemplo, consulte [Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades \(p. 847\)](#).

Sob demanda na frota spot

Para garantir que você sempre tenha capacidade de instância, você pode incluir uma solicitação de capacidade sob demanda na solicitação de frota spot. Na solicitação de frota spot, especifique a capacidade desejada de destino e a quantidade dessa capacidade que deve ser sob demanda. O saldo compromete a capacidade spot, que será executada se houver capacidade e disponibilidade do Amazon EC2 disponíveis. Por exemplo, se você especificar na solicitação de frota spot a capacidade pretendida como 10 e a capacidade sob demanda como 8, o Amazon EC2 executará 8 unidades de capacidade como sob demanda e 2 unidades de capacidade ($10 - 8 = 2$) como spot.

Priorizar tipos de instâncias para capacidade sob demanda

Quando a frota spot tenta atender à sua capacidade sob demanda, o padrão é iniciar primeiro o tipo de instância de menor preço. Se `OnDemandAllocationStrategy` estiver definido como `prioritized`, a frota spot usará a prioridade para determinar qual tipo de instância será o primeiro para atender a capacidade sob demanda. A prioridade é atribuída à substituição do modelo de ativação, e a prioridade mais alta é lançada primeiro.

Por exemplo, você configurou três substituições de modelo de ativação, cada uma com um tipo de instância diferente: `c3.large`, `c4.large` e `c5.large`. O preço sob demanda para `c5.large` é menor do que para `c4.large`. `c3.large` é o mais barato. Se você não usar a prioridade para determinar o pedido, a frota atenderá à capacidade sob demanda começando com `c3.large` e, em seguida, `c5.large`. Como, muitas vezes, há Instâncias reservadas não usados para `c4.large`, você pode definir a prioridade de substituição do modelo de ativação para que a ordem seja `c4.large`, `c3.large` e `c5.large`.

Rebalanceamento de capacidade

Você pode configurar a frota spot para iniciar uma instância spot de substituição quando o Amazon EC2 emitir uma recomendação de rebalanceamento para notificar que uma instância spot está em um risco elevado de interrupção. O rebalanceamento de capacidade ajuda a manter a disponibilidade da workload aumentando proativamente sua frota com uma nova instância spot antes que uma instância em execução seja interrompida por Amazon EC2. Para obter mais informações, consulte [Recomendações de rebalanceamento de instâncias do EC2 \(p. 333\)](#).

Para configurar a frota spot para iniciar uma instância spot de substituição, você pode usar o console do Amazon EC2 ou a AWS CLI.

- Console do Amazon EC2: marque a caixa de seleção Capacity rebalance (Rebalancear capacidade) ao criar a frota spot. Para obter mais informações, consulte a etapa 6.d em [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 777\)](#).
- AWS CLI: use o comando `request-spot-fleet` e os parâmetros relevantes na estrutura da `SpotMaintenanceStrategies`. Para obter mais informações, consulte o [exemplo de configuração de execução \(p. 846\)](#).

Limitações

- Disponível apenas para frotas do tipo `maintain`.

- Quando a frota estiver em execução, não é possível modificar a configuração de rebalanceamento de capacidade. Para alterar a configuração de rebalanceamento de capacidade, você deve excluir a frota e criar uma nova.

Considerações

Se você configurar uma frota spot para rebalanceamento de capacidade, considere o seguinte:

A frota spot pode executar a nova instâncias spot de substituição até que a capacidade satisfeita seja a capacidade dobro de destino

Quando uma frota spot é configurada para rebalanceamento de capacidade, a frota tenta executar uma nova instância spot de substituição para cada instância spot que recebe uma recomendação de rebalanceamento. Depois que uma instância spot receber uma recomendação de rebalanceamento, ela não é mais contada como parte da capacidade de atendimento e a frota spot não encerra automaticamente a instância. Isso dá a você a oportunidade de executar [ações de rebalanceamento \(p. 334\)](#) na instância. Depois disso, você pode encerrar a instância ou deixá-la em execução.

Se sua frota atingir o dobro da capacidade de destino, ela interrompe a execução de novas instâncias de substituição, mesmo que as próprias instâncias de substituição recebam uma recomendação de rebalanceamento.

Por exemplo, você cria uma frota spot com uma capacidade de destino de 100 instâncias spot. Todas as instâncias spot recebem uma recomendação de rebalanceamento, o que faz com que a frota spot execute 100 instâncias spot substitutas. Isso eleva o número de instâncias spot atendidas para 200, o que é o dobro da capacidade de destino. Algumas das instâncias de substituição recebem uma recomendação de rebalanceamento, porém nenhuma instância de substituição é executada porque a frota não pode exceder o dobro da capacidade de destino.

Observe que você é cobrado por todas as instâncias durante a execução.

Recomendamos que você encerre manualmente as instâncias spot que recebem uma recomendação de rebalanceamento

Se você configurar a frota spot para rebalanceamento de capacidade, recomendamos que você monitore o sinal de recomendação de rebalanceamento recebido pelas instâncias spot na frota. Ao monitorar o sinal, você pode executar rapidamente [ações de rebalanceamento \(p. 334\)](#) nas instâncias afetadas, antes que o Amazon EC2 as interrompa e, em seguida, você pode encerrá-las manualmente. Se você não encerrar as instâncias, continuará pagando por elas enquanto estiverem em execução. A frota spot não encerra automaticamente as instâncias que recebem uma recomendação de rebalanceamento.

Você pode configurar notificações usando o Amazon EventBridge ou metadados da instância. Para obter mais informações, consulte [Monitorar os sinais de recomendação de rebalanceamento \(p. 334\)](#).

A frota spot não conta as instâncias que recebem uma recomendação de rebalanceamento ao calcular a capacidade atendida durante o aumento ou a diminuição

Se a frota spot estiver configurada para rebalanceamento de capacidade e você alterar a capacidade de destino para aumento ou diminuição, a frota não contará as instâncias marcadas para rebalanceamento como parte da capacidade atendida, como a seguir:

- Diminuição – Se você diminuir a capacidade de destino desejada, a frota encerrará instâncias que não estão marcadas para rebalanceamento até que a capacidade desejada seja atingida. As instâncias marcadas para reequilíbrio não são contabilizadas para a capacidade atendida.

Por exemplo, você cria uma frota spot com uma capacidade planejada de 100 instâncias spot.

10 instâncias recebem uma recomendação de rebalanceamento, portanto, a frota inicia 10 novas instâncias de substituição, resultando em uma capacidade atendida de 110 instâncias. Em seguida,

você reduz a capacidade de destino para 50 (diminuição), mas a capacidade de atendimento é, na verdade, 60 instâncias porque as 10 instâncias marcadas para rebalanceamento não são encerradas pela frota. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

- Aumento – Se você aumentar a capacidade desejada, a frota iniciará novas instâncias até que a capacidade desejada seja atingida. As instâncias marcadas para reequilíbrio não são contabilizadas para a capacidade atendida.

Por exemplo, você cria uma frota spot com uma capacidade planejada de 100 instâncias spot. 10 instâncias recebem uma recomendação de rebalanceamento, portanto, a frota inicia 10 novas instâncias de substituição, resultando em uma capacidade atendida de 110 instâncias. Em seguida, você aumenta a capacidade de destino para 200 (aumento), mas a capacidade de atendimento é, na verdade, 210 instâncias porque as 10 instâncias marcadas para rebalanceamento não são contabilizadas pela frota como parte da capacidade de destino. Você precisa encerrar manualmente essas instâncias ou deixá-las em execução.

Forneça o maior número possível de grupos de capacidade spot na solicitação

Configure sua frota spot para usar vários tipos de instância e zonas de disponibilidade. Isso oferece a flexibilidade para executar instâncias spot em vários grupos de capacidade spot. Para obter mais informações, consulte [Ser flexível sobre tipos de instância e zonas de disponibilidade \(p. 303\)](#).

Configure sua frota spot para usar os grupos de capacidade spot mais adequados

Use a estratégia de alocação de `capacity-optimized` para garantir que as instâncias spot de substituição sejam executadas nos grupos de capacidade spot mais adequados. Para obter mais informações, consulte [Usar a estratégia de alocação otimizada por capacidade \(p. 304\)](#).

Substituições do preço spot

Cada solicitação de frota spot pode incluir um preço máximo global ou usar o padrão (preço sob demanda). A frota spot usa esse preço como o preço máximo padrão em cada uma das suas especificações de execução.

É possível especificar um preço máximo em uma ou mais especificações de execução. Esse preço é específico da especificação de execução. Se uma especificação de execução incluir um preço específico, a frota spot usará esse preço máximo para substituir o preço máximo global. Qualquer outra especificação de execução que não inclua um preço máximo específico ainda usará o preço máximo global.

Controle de gastos

A frota spot para de executar instâncias quando atinge a capacidade de destino ou o valor máximo que você está disposto a pagar. Para controlar a quantidade paga por hora da sua frota, especifique o `SpotMaxTotalPrice` para o Instâncias spot e o `OnDemandMaxTotalPrice` para Instâncias on-demand. Quando o preço total máximo for alcançado, a frota spot para de iniciar instâncias mesmo que não tenha atingido a capacidade alvo.

Os exemplos a seguir mostram duas situações diferentes. Na primeira, a frota spot para de executar instâncias ao atingir a capacidade de destino. Na segunda, a frota spot para de executar instâncias ao atingir o valor máximo que você está disposto a pagar.

Exemplo: parar de executar instâncias quando a capacidade de destino for atingida

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 1,50 USD

A frota spot executa 10 Instâncias sob demanda, porque o total de 1,00 USD (10 instâncias x 0,10 USD) não excede o `OnDemandMaxTotalPrice` de 1,50 USD.

Exemplo: parar de executar instâncias quando o preço máximo total for atingido

Dada uma solicitação de `m4.large` Instâncias on-demand, na qual:

- Preço sob demanda: 0,10 USD por hora
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 0,80 USD

Se a frota spot executar a capacidade planejada (10 Instâncias on-demand), o custo total por hora será de 1,00 USD. Isso é mais que a quantidade (0,80 USD) especificada para `OnDemandMaxTotalPrice`. Para evitar gastar mais do que você pretende, a frota spot abre somente oito instâncias sob demanda (abaixo da capacidade de destino sob demanda), porque abrir mais excederia o `OnDemandMaxTotalPrice`.

Peso de instâncias de frotas spot

Ao solicitar uma frota de Instâncias spot, você poderá definir as unidades de capacidade com que cada tipo de instância contribuirá para a performance da aplicação e poderá ajustar corretamente o preço máximo para cada grupo de capacidade spot usando o peso da instância.

Por padrão, o preço que você especifica é por hora de instância. Ao usar o recurso de peso da instância, o preço que você especifica é por hora. Você pode calcular o preço por hora dividindo seu preço para um tipo de instância pelo número de unidades que ele representa. A frota spot calcula o número de instâncias spot a serem executadas dividindo a capacidade de destino pelo peso da instância. Se o resultado não for um valor inteiro, a frota spot o arredondará para o próximo valor inteiro, para que o tamanho de sua frota não fique abaixo de sua capacidade de destino. A frota spot pode selecionar qualquer grupo que você determinar na especificação de execução, mesmo que a capacidade das instâncias executadas ultrapasse a capacidade de destino solicitada.

As tabelas a seguir fornecem exemplos de cálculos para determinar o preço por unidade para uma solicitação de frota spot com capacidade de destino igual a 10.

Tipo de instância	Peso da instância	Preço por hora de instância	Preço por hora	Número de instâncias executadas
<code>r3.xlarge</code>	2	0,05 USD	0,025 (0,05 dividido por 2)	5 (10 dividido por 2)

Tipo de instância	Peso da instância	Preço por hora de instância	Preço por hora	Número de instâncias executadas
<code>r3.8xlarge</code>	8	0,10 USD	0,0125 (0,10 dividido por 8)	2 (10 dividido por 8, resultado arredondado para cima)

Use o peso de instância de frotas spot da maneira a seguir para provisionar a capacidade planejada nos grupos com o menor preço por unidade no momento do atendimento:

1. Defina a capacidade planejada da frota spot em instâncias (o padrão) ou nas unidades de sua preferência, como CPUs virtuais, memória, armazenamento ou taxa de transferência.

2. Defina o preço por unidade.
3. Para cada configuração de execução, especifique o peso, que é o número de unidades que o tipo de instância representa em relação à capacidade de destino.

Exemplo de peso da instância

Considere uma solicitação de frota spot com a seguinte configuração:

- Uma capacidade de destino de 24
- Uma especificação de execução com um tipo de instância `r3.2xlarge` e um peso de 6
- Uma especificação de execução com um tipo de instância `c3.xlarge` e um peso de 5

Os pesos representam o número de unidades que o tipo de instância representa em relação à capacidade de destino. Se a primeira especificação de execução fornecer o menor preço por unidade (preço de `r3.2xlarge` por hora de instância dividido por 6), a frota spot executará quatro dessas instâncias (24 dividido por 6).

Se a segunda especificação de execução fornecer o menor preço por unidade (preço de `c3.xlarge` por hora de instância dividido por 5), a frota spot executará cinco dessas instâncias (24 dividido por 5, resultado arredondado para cima).

Peso da instância e estratégia de alocação

Considere uma solicitação de frota spot com a seguinte configuração:

- Uma capacidade de destino de 30
- Uma especificação de execução com um tipo de instância `c3.2xlarge` e um peso de 8
- Uma especificação de execução com um tipo de instância `m3.xlarge` e um peso de 8
- Uma especificação de execução com um tipo de instância `r3.xlarge` e um peso de 8

A frota spot executará quatro instâncias (30 dividido por 8, resultado arredondado para cima). Com a estratégia `lowestPrice`, todas as quatro instâncias vêm do grupo que fornece o menor preço por unidade. Com a estratégia `diversified`, a frota spot executa uma instância em cada um dos três grupos, e a quarta instância em qualquer grupo que forneça o menor preço por unidade.

Trabalhar com frotas spot

Para começar a usar uma frota spot, crie uma solicitação de frota spot que inclua a capacidade pretendida, uma parte opcional sob demanda, uma ou mais especificações de lançamento para as instâncias e o preço máximo que você está disposto a pagar. O solicitação de frota deve incluir um modelo de lançamento que defina as informações de que a frota precisa para iniciar uma instância, como uma AMI, um tipo de instância, uma sub-rede ou uma zona de disponibilidade e um ou mais grupos de segurança.

Se a frota incluir a Instâncias spot, o Amazon EC2 pode tentar manter a capacidade pretendida da frota quando os preços spot forem alterados.

Não é possível modificar a capacidade de destino de uma solicitação única depois que ela for enviada. Para alterar a capacidade de destino, cancele a solicitação e envie uma nova.

Uma solicitação de frota spot permanecerá ativa até que expire ou você a cancele. Ao cancelar uma solicitação de frota spot, você pode especificar se esse cancelamento da solicitação encerra as instâncias spot nessa frota spot.

Tópicos

- [Estados das solicitações de frota spot \(p. 770\)](#)

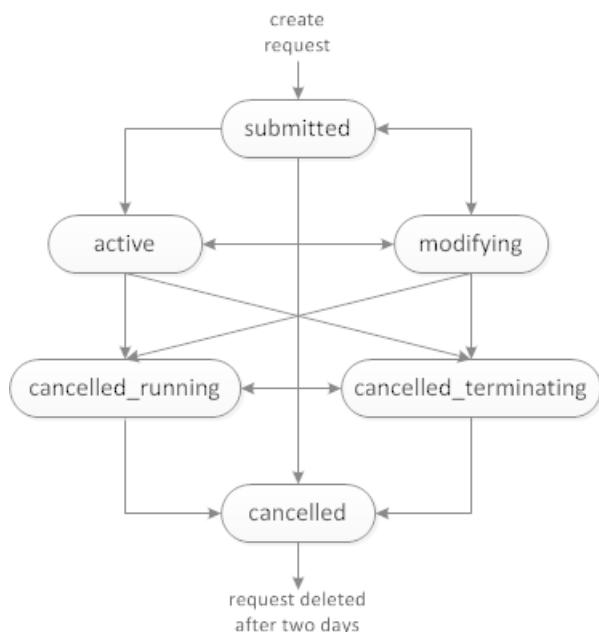
- Verificações de integridade da frota spot (p. 771)
 - Permissões de frota spot (p. 771)
 - Criar uma solicitação de frota spot (p. 776)
 - Marcar uma frota spot (p. 780)
 - Monitorar sua frota spot (p. 787)
 - Modificar uma solicitação de frota spot (p. 787)
 - Cancelar uma solicitação de frota spot (p. 789)

Estados das solicitações de frota spot

Uma solicitação de frota spot pode estar em um dos seguintes estados:

- **submitted**: a solicitação de frota spot está sendo avaliada, e o Amazon EC2 está se preparando para executar o número pretendido de instâncias.
 - **active**: a frota spot foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias spot em execução. A solicitação permanece nesse estado até que seja alterada ou cancelada.
 - **modifying**: a solicitação de frota spot está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada ou até que a frota spot seja cancelada. Uma request única não pode ser alterada, e esse estado não se aplica a essas solicitações spot.
 - **cancelled_running**: a frota spot foi cancelada e não executa instâncias spot adicionais. Suas Instâncias spot existentes continuam sendo executadas até que sejam interrompidas ou encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas.
 - **cancelled_terminating**: a frota spot é cancelada e suas instâncias spot estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.
 - **cancelled**: a frota spot é cancelada e não tem instâncias spot em execução. A solicitação de frota spot foi excluída dois dias depois que as instâncias foram encerradas.

A ilustração a seguir representa as transições entre os estados da solicitação. Se você exceder os limites da frota spot, a solicitação será cancelada imediatamente.



Verificações de integridade da frota spot

A frota spot verifica o status de integridade das instâncias spot na frota a cada dois minutos. O status de integridade de uma instância é `healthy` ou `unhealthy`.

A frota spot determina o status de integridade de uma instância usando as verificações de status fornecidas pelo Amazon EC2. Uma instância é determinada como `unhealthy` quando o status da verificação de status da instância ou da verificação de status do sistema for `impaired` para três verificações de integridade consecutivas. Para obter mais informações, consulte [Verificações de status para as instâncias \(p. 867\)](#).

Você pode configurar a sua frota para substituir Instâncias spot não íntegras. Depois de habilitar a substituição da verificação de integridade, uma instância spot é substituída ao ser relatada como `unhealthy`. A frota pode ficar abaixo de sua capacidade de destino por até alguns minutos enquanto uma instância spot não íntegra está sendo substituída.

Requirements

- A substituição da verificação de integridade é compatível apenas para Frotas spot que mantenham uma capacidade de destino (frotas do tipo `maintain`) e não para Frotas spot únicas (frotas do tipo `request`).
- A substituição da verificação de integridade é compatível apenas para Instâncias spot. Este recurso não é compatível para Instâncias on-demand.
- Você pode configurar a frota spot para substituir instâncias não íntegras somente durante sua criação.
- Os usuários do IAM poderão usar a substituição de verificação de integridade somente se tiverem permissão para chamar a ação `ec2:DescribeInstanceStatus`.

Console

Para configurar uma frota spot para substituir instâncias spot não íntegras usando o console

1. Siga as etapas para criar um frota spot. Para obter mais informações, consulte [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 777\)](#).
2. Para configurar a frota para substituir Instâncias spot não íntegras para a Health check (Verificação de integridade), selecione Replace unhealthy instances (Substituir instâncias não íntegras). Para habilitar essa opção, primeiramente você deve selecionar Maintain target capacity (Manter capacidade de destino).

AWS CLI

Para configurar uma frota spot para substituir instâncias spot não íntegras usando a AWS CLI

1. Siga as etapas para criar um frota spot. Para obter mais informações, consulte [Criar uma frota spot usando a AWS CLI \(p. 780\)](#).
2. Para configurar a frota para substituir Instâncias spot não íntegras, para `ReplaceUnhealthyInstances`, insira `true`.

Permissões de frota spot

Se os usuários do IAM vão criar ou gerenciar uma frota spot, é necessário conceder a eles as permissões necessárias.

Se você usar o console do Amazon EC2 para criar uma frota spot, ele criará duas funções vinculada ao serviço chamadas `AWSServiceRoleForEC2SpotFleet` e `AWSServiceRoleForEC2Spot`, e uma função chamada `aws-ec2-spot-fleet-tagging-role` que concede à frota spot as permissões de

para solicitar, executar, encerrar e marcar recursos em seu nome. Se você usar a AWS CLI ou uma API, é necessário garantir que essas funções existam.

Use as instruções a seguir para conceder as permissões necessárias e criar as funções.

Permissões e funções

- [Conceder aos usuários do IAM a permissão para a frota spot \(p. 772\)](#)
- [Função vinculada ao serviço para frota spot \(p. 774\)](#)
- [Função vinculada ao serviço para instâncias spot \(p. 775\)](#)
- [Função do IAM para marcar uma frota spot \(p. 776\)](#)

Conceder aos usuários do IAM a permissão para a frota spot

Se os usuários do IAM vão criar ou gerenciar uma frota spot, certifique-se de conceder a eles as permissões necessárias da maneira a seguir.

Para conceder aos usuários do IAM as permissões para a frota spot

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Policies, Create policy.
3. Na página Criar política, selecione JSON, e substitua o texto pelo indicado a seguir.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances",  
                "ec2:CreateTags",  
                "ec2:RequestSpotFleet",  
                "ec2:ModifySpotFleetRequest",  
                "ec2:CancelSpotFleetRequests",  
                "ec2:DescribeSpotFleetRequests",  
                "ec2:DescribeSpotFleetInstances",  
                "ec2:DescribeSpotFleetRequestHistory"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "iam:PassRole",  
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "iam>CreateServiceLinkedRole",  
                "iam>ListRoles",  
                "iam>ListInstanceProfiles"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

A política de exemplo anterior concede a um usuário do IAM as permissões necessárias para a maioria dos casos de uso de frota spot. Para limitar o usuário a ações de API específicas, especifique somente essas ações de API.

APIs do EC2 e do IAM necessárias

As seguintes APIs devem ser incluídas na política:

- `ec2:RunInstances`: necessária para executar instâncias em uma frota spot
- `ec2:CreateTags`: necessária para marcar as solicitações, instâncias ou volumes de frota spot
- `iam:PassRole`: necessária para especificar a função da frota spot
- `iam>CreateServiceLinkedRole`: necessária para criar a função vinculada ao serviço
- `iam>ListRoles`: necessária para enumerar funções do IAM existentes
- `iam>ListInstanceProfiles`: necessária para enumerar perfis de instância existentes

Important

Se você especificar uma função para o perfil de instância do IAM na especificação de execução ou no modelo de execução, deverá conceder ao usuário do IAM a permissão para passar a função para o serviço. Para fazer isso, na política do IAM inclua "`arn:aws:iam::*:role/IamInstanceProfile-role`" como um recurso para a ação `iam:PassRole`. Para obter mais informações, consulte [Granting a user permissions to pass a role to an AWS service](#) (Conceder permissões ao usuário para passar uma função a um produto da AWS) no IAM User Guide (Manual do usuário do IAM).

APIs de frota spot

Adicione as seguintes ações da API de frota spot à política, conforme necessário:

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

APIs opcionais do IAM

(Opcional) Para permitir que um usuário do IAM crie funções ou perfis de instância usando o console do IAM, é necessário adicionar as seguintes ações à política:

- `iam:AddRoleToInstanceProfile`
 - `iam:AttachRolePolicy`
 - `iam>CreateInstanceProfile`
 - `iam>CreateRole`
 - `iam:GetRole`
 - `iam>ListPolicies`
4. Escolha Revisar política.
 5. Na página Review policy (Revisar política), digite um nome e uma descrição para a política e escolha Create policy (Criar política).
 6. No painel de navegação, escolha Users (Usuários) e selecione o usuário.
 7. Selecione Permissions e Add permissions.
 8. Selecione Attach existing policies directly. Selecione a política que você criou anteriormente e escolha Next: Review (Próximo: Revisão).
 9. Selecione Add permissions.

Função vinculada ao serviço para frota spot

O Amazon EC2 usa funções vinculadas ao serviço para as permissões de que ela precisa para chamar outros produtos da AWS em seu nome. Uma função vinculada ao serviço é um tipo exclusivo de função do IAM que é vinculado diretamente a um produto da AWS. As funções vinculadas a serviços oferecem uma maneira segura de delegar permissões a serviços da AWS, pois somente o serviço vinculado pode assumir uma função vinculada ao serviço. Para obter mais informações, consulte [Uso de funções vinculadas ao serviço](#) no Guia do usuário do IAM.

O Amazon EC2 usa a função vinculada ao serviço chamada AWSServiceRoleForEC2SpotFleet para executar e gerenciar instâncias em seu nome.

Important

Se você especificar uma [AMI criptografada \(p. 135\)](#) ou um [snapshot criptografado do Amazon EBS \(p. 1422\)](#) na frota spot, será necessário conceder à função AWSServiceRoleForEC2SpotFleet permissão para usar a CMK a fim de que o Amazon EC2 possa executar instâncias em seu nome. Para obter mais informações, consulte [Conceder acesso às CMKs para uso com AMIs criptografadas e snapshots do EBS \(p. 775\)](#).

Permissões concedidas por AWSServiceRoleForEC2SpotFleet

O Amazon EC2 usa AWSServiceRoleForEC2SpotFleet para concluir as ações a seguir:

- `ec2:RequestSpotInstances` - Solicitar Instâncias spot
- `ec2:RunInstances` - executar instâncias
- `ec2:TerminateInstances` - encerrar instâncias
- `ec2:DescribeImages` - descrever imagens de máquina da Amazon (AMIs) para as instâncias
- `ec2:DescribeInstanceStatus` - descrever o status das instâncias
- `ec2:DescribeSubnets` – descrever as sub-redes das instâncias
- `ec2>CreateTags`: adiciona tags à solicitação, às instâncias e aos volumes de frota spot
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` - adicionar as instâncias especificadas ao load balancer especificado.
- `elasticloadbalancing:RegisterTargets` - registrar os destinos especificados no grupo de destino especificado.

Criar a função vinculada ao serviço

Na maioria das circunstâncias, você não precisa criar manualmente uma função vinculada ao serviço. O Amazon EC2 cria a função AWSServiceRoleForEC2SpotFleet vinculada ao serviço na primeira vez que você criar uma frota spot usando o console.

Se você tinha uma solicitação de frota spot ativa antes de outubro de 2017, quando o Amazon EC2 começou a oferecer suporte a essa função vinculada ao serviço, o Amazon EC2 criou a função AWSServiceRoleForEC2SpotFleet em sua conta da AWS. Para obter mais informações, consulte [A new role appeared in my AWS account](#) (Uma nova função apareceu na minha conta da AWS) no IAM User Guide (Manual do usuário do IAM).

Se você usar a AWS CLI ou uma API para criar uma frota spot, deverá assegurar que essa função existe.

Para criar AWSServiceRoleForEC2SpotFleet usando o console

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, selecione Roles.
3. Selecione Create role.
4. Em Select type of trusted entity (Selecionar tipo de entidade confiável), escolha AWS service (Produto da AWS).

5. Em Choose a use case (Escolha um caso de uso), Or select a service to view its use cases (Ou selecione um serviço para visualizar seus casos de uso), escolha EC2.
6. Em Select your use case (Seleciona seu caso de uso), escolha EC2 - Spot Fleet (EC2 - Frota spot).
7. Escolha Próximo: Permissões.
8. Na próxima página, escolha Next: Tags (Próximo: tags).
9. Na próxima página, escolha Next: Review (Próximo: revisão).
10. Na página Review (Revisar), selecione Create role (Criar função).

Para criar AWSServiceRoleForEc2SpotFleet usando o AWS CLI

Use o comando [create-service-linked-role](#) da seguinte forma.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Se você não precisar mais usar a frota spot, é recomendável excluir a função AWSServiceRoleForEC2SpotFleet. Depois que a função for excluída da conta, o Amazon EC2 criará a função novamente se você solicitar uma frota spot usando o console. Para obter mais informações, consulte [Excluir uma função vinculada ao serviço](#) no Guia do usuário do IAM.

Conceder acesso às CMKs para uso com AMIs criptografadas e snapshots do EBS

Se você especificar uma [AMI criptografada \(p. 135\)](#) ou um [snapshot do Amazon EBS criptografado \(p. 1422\)](#) na solicitação de frota spot e usar uma chave mestra do cliente (CMK) gerenciada pelo cliente para criptografia, deverá conceder à função AWSServiceRoleForEC2SpotFleet permissão para usar a CMK de forma que o Amazon EC2 consiga executar instâncias em seu nome. Para isso, adicione uma concessão à CMK, conforme exibido no procedimento a seguir.

Durante a definição de permissões, as concessões são uma alternativa às políticas de chave. Para obter mais informações, consulte [Using grants \(Usar concessões\)](#) e [Using key policies in AWS KMS \(Usar políticas de chave no AWS KMS\)](#) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

Para conceder à função AWSServiceRoleForEC2SpotFleet permissões para usar a CMK

- Use o comando [create-grant](#) para adicionar uma concessão à CMK e especificar a entidade principal (a função vinculada ao serviço AWSServiceRoleForEC2SpotFleet) que recebe permissão para executar as operações permitidas pela concessão. A CMK é especificada pelo parâmetro `key-id` e pelo ARN da CMK. A entidade principal é especificada pelo parâmetro `grantee-principal` e pelo ARN da função vinculada ao serviço AWSServiceRoleForEC2SpotFleet.

```
aws kms create-grant \
  --region us-east-1 \
  --key-id arn:aws:kms:us-
east-1:44445556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
  --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2SpotFleet \
  --operations "Decrypt" "Encrypt" "GenerateDataKey"
  "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
  "ReEncryptTo"
```

Função vinculada ao serviço para instâncias spot

O Amazon EC2 usa a função vinculada ao serviço denominada AWSServiceRoleForEC2Spot para executar e gerenciar Instâncias spot em seu nome. Para obter mais informações, consulte [Função vinculada ao serviço para solicitações de instâncias spot \(p. 311\)](#).

Função do IAM para marcar uma frota spot

A função do IAM `aws-ec2-spot-fleet-tagging-role` concede à frota spot permissão para marcar a solicitação, as instâncias e os volumes de frota spot. Para obter mais informações, consulte [Marcar uma frota spot \(p. 780\)](#).

Important

Se você optar por marcar instâncias na frota e por manter a capacidade de destino (a solicitação de frota spot é do tipo `maintain`), as diferenças nas permissões do usuário do IAM e da `IamFleetRole` poderão levar a um comportamento inconsistente de marcação das instâncias na frota. Se o `IamFleetRole` não incluir a permissão `CreateTags`, algumas das instâncias executadas pela frota não serão marcadas. Embora estejamos trabalhando para corrigir essa inconsistência, para garantir que todas as instâncias executadas pela frota sejam marcadas, recomendamos que você use a função `aws-ec2-spot-fleet-tagging-role` para `IamFleetRole`. Outra opção é para usar uma função existente, anexe a `AmazonEC2SpotFleetTaggingRolePolítica` gerenciada da AWS à função existente. Caso contrário, você precisará adicionar manualmente a permissão `CreateTags` à política existente.

Para criar uma função do IAM para marcar uma frota spot

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, selecione Roles.
3. Selecione Create roles (Criar funções).
4. Na página Select type of trusted entity (Selecionar tipo de entidade confiável), escolha AWS service (Produto da AWS).
5. Em Choose a use case (Escolha um caso de uso), Or select a service to view its use cases (Ou selecione um serviço para visualizar seus casos de uso), escolha EC2.
6. Em Select your use case (Selecionar seu caso de uso), escolha EC2 - Spot Fleet Tagging (EC2 - Marcação de frota spot).
7. Escolha Próximo: Permissões.
8. Na próxima página, escolha Next: Tags (Próximo: tags).
9. Na próxima página, escolha Next: Review (Próximo: revisão).
10. Na página Review (Revisar), digite um nome para a função (por exemplo, `aws-ec2-spot-fleet-tagging-role`) e selecione Create role (Criar função).

Criar uma solicitação de frota spot

Usando o AWS Management Console, crie rapidamente uma solicitação de frota spot escolhendo apenas a aplicação ou tarefa necessária e as especificações mínimas de computação. O Amazon EC2 configura uma frota que melhor atenda às suas necessidades e siga a prática recomendada de spot. Para obter mais informações, consulte [Criar uma solicitação de frota spot rapidamente \(console\) \(p. 776\)](#). Caso contrário, você pode modificar qualquer uma das configurações padrão. Para obter mais informações, consulte [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 777\)](#) e [Criar uma frota spot usando a AWS CLI \(p. 780\)](#).

Opções para criar uma frota spot

- [Criar uma solicitação de frota spot rapidamente \(console\) \(p. 776\)](#)
- [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 777\)](#)
- [Criar uma frota spot usando a AWS CLI \(p. 780\)](#)

Criar uma solicitação de frota spot rapidamente (console)

Siga estas etapas para criar rapidamente uma solicitação de frota spot.

Para criar uma solicitação de frota spot usando as configurações recomendadas (console)

1. Abra o console Spot em <https://console.aws.amazon.com/ec2spot>.
2. Se você estiver começando a usar spot, verá uma página de boas-vindas. Escolha Comece a usar. Caso contrário, selecione Solicitar Instâncias spot.
3. Em Tell us your application or task need (Informe a necessidade de sua aplicação ou tarefa), escolha Load balancing workloads (Workloads de balanceamento de carga), Flexible workloads (Workloads flexíveis) ou Big data workloads (Workloads de big data).
4. Em Configure your instances (Configurar suas instâncias), em Minimum compute unit (Unidade mínima de computação), escolha as especificações mínimas de hardware (vCPUs, memória e armazenamento) necessárias para a aplicação ou tarefa, as specs (como especificações) ou as an instance type (como um tipo de instância).
 - Em as specs (como especificações), especifique o número necessário de vCPUs e a quantidade de memória.
 - Em as an instance type (como um tipo de instância), aceite o tipo de instância padrão ou escolha Change instance type (Alterar tipo de instância) para escolher outro tipo de instância.
5. Em Tell us how much capacity you need (Informe a quantidade de capacidade necessária), em Total target capacity (Capacidade total de destino), especifique o número de unidades a serem solicitadas para a capacidade de destino. Você pode escolher instâncias ou vCPUs.
6. Reveja as Fleet request settings (Configurações de solicitação de frota) com base na seleção de sua aplicação ou tarefa e escolha Launch (Executar).

Criar uma solicitação de frota spot usando parâmetros definidos (console)

Você pode criar uma frota spot usando parâmetros definidos por você.

Para criar uma solicitação de frota spot usando parâmetros definidos (console)

1. Abra o console Spot em <https://console.aws.amazon.com/ec2spot>.
2. Se você estiver começando a usar spot, verá uma página de boas-vindas. Escolha Comece a usar. Caso contrário, selecione Solicitar Instâncias spot.
3. Em Tell us your application or task need (Informe a necessidade de sua aplicação ou tarefa), escolha Load balancing workloads (Workloads de balanceamento de carga), Flexible workloads (Workloads flexíveis) ou Big data workloads (Workloads de big data).
4. Em Configure your instances (Configurar suas instâncias), faça o seguinte:
 - a. (Opcional) Para Launch template, escolha um modelo de execução. O modelo de execução deve especificar uma Imagem de máquina da Amazon (AMI), pois não será possível substituir a AMI usando a frota spot se você especificar um modelo de execução.

Important

Se você pretender especificar Optional On-Demand portion (Parte opcional sob demanda), deverá escolher um modelo de execução.

- b. Em AMI, escolha uma das AMIs básicas fornecidas pela AWS ou escolha Search for AMI (Pesquisar AMI) para usar uma AMI de nossa comunidade de usuários, do AWS Marketplace ou uma própria.
- c. Em Minimum compute unit (Unidade mínima de computação), escolha as especificações mínimas de hardware (vCPUs, memória e armazenamento) necessárias para a aplicação ou tarefa, as specs (como especificações) ou as an instance type (como um tipo de instância).
 - Em as specs (como especificações), especifique o número necessário de vCPUs e a quantidade de memória.

- Em as an instance type (como um tipo de instância), aceite o tipo de instância padrão ou escolha Change instance type (Alterar tipo de instância) para escolher outro tipo de instância.
- d. Em Rede, escolha uma VPC existente ou crie uma nova.

[VPC existente] escolha a VPC.

[VPC nova] Escolha Create new VPC (Criar nova VPC) para acessar o console da Amazon VPC. Ao concluir, volte para o assistente e atualize a lista.

- e. (Opcional) Em Availability Zones (Zonas de disponibilidade), deixe que a AWS escolha as zonas de disponibilidade para suas instâncias spot ou especifique uma ou mais zonas de disponibilidade.

Se houver mais de uma sub-rede em uma zona de disponibilidade, escolha a sub-rede apropriada em Subnet (Sub-rede). Para adicionar sub-redes, escolha Create new subnet (Criar nova sub-rede) para acessar o console da Amazon VPC. Ao concluir, volte para o assistente e atualize a lista.

- f. (Opcional) Em Key pair name (Nome do par de chaves), escolha um par de chaves existente ou crie uma novo.

[Par de chaves existente] Escolha o par de chaves.

[Novo par de chaves] Escolha Create new key pair (Criar novo par de chaves) para acessar o console da Amazon VPC. Ao concluir, volte para o assistente e atualize a lista.

- 5. (Opcional) Em Additional configurations (Configurações adicionais), faça o seguinte:

- a. (Opcional) Para habilitar a otimização de Amazon EBS, em EBS-optimized (Otimizada para EBS), escolha Launch EBS-optimized instances (Executar instâncias otimizadas para EBS).
- b. (Opcional) Para adicionar armazenamento temporário em nível de blocos para suas instâncias, em Instance store (Armazenamento de instâncias), escolha Attach at launch (Anexar na execução).
- c. (Opcional) Para adicionar armazenamento, especifique volumes de armazenamento de instâncias ou volumes do Amazon EBS adicionais, dependendo do tipo de instância.
- d. (Opcional) Por padrão, o monitoramento básico está habilitado para suas instâncias. Para habilitar o monitoramento detalhado, em Monitoring (Monitoramento), escolha Enable CloudWatch detailed monitoring (Habilitar monitoramento detalhado do).
- e. (Optional) Para substituir Instâncias spot não íntegras, para a Health check (Verificação de integridade), escolha Replace unhealthy instances (Substituir instâncias não íntegras). Para habilitar essa opção, primeiramente você deve selecionar Maintain target capacity (Manter capacidade de destino).
- f. (Opcional) Para executar uma instância spot dedicada, em Tenancy (Locação), selecione em Dedicated - run a dedicated instance (Dedicada: executar uma instância dedicada).
- g. (Opcional) Em Security groups (Grupos de segurança), escolha um ou mais grupos de segurança ou crie um novo.

[Grupo de segurança existente] Escolha um ou mais grupos de segurança.

[Novo grupo de segurança] Escolha Create a new security group (Criar um novo grupo de segurança) para acessar o console da Amazon VPC. Ao concluir, volte para o assistente e atualize a lista.

- h. (Opcional) Para tornar as instâncias acessíveis na Internet, em Auto-assign IPv4 Public IP (Atribuir automaticamente IP público IPv4), escolha Enable (Habilitar).
- i. (Opcional) Para executar as Instâncias spot com uma função do IAM, em IAM instance profile (Perfil de instância do IAM), escolha a função.
- j. (Opcional) Para executar um script de startup, copie-o para User data.

- k. (Opcional) Para adicionar uma tag, escolha Add new tag (Adicionar nova tag) e digite a chave e o valor da tag. Repita esse procedimento para cada tag.

Para cada etiqueta, para marcar as instâncias e a solicitação de frota spot com a mesma etiqueta, verifique se Instância e Frota estão ambas selecionadas. Para marcar apenas as instâncias iniciadas pela frota, desmarque Frota. Para marcar apenas a solicitação de frota spot, desmarque Instância.

6. Em Tell us how much capacity you need (Informe a quantidade de capacidade necessária), faça o seguinte:

- a. Em Total target capacity (Capacidade total de destino), especifique o número de unidades a serem solicitadas para a capacidade de destino. Você pode escolher instâncias ou vCPUs. Para especificar uma capacidade de destino igual a 0 para que seja possível adicionar capacidade posteriormente, escolha Maintain target capacity (Manter a capacidade do destino).
- b. (Opcional) Em Optional On-Demand portion (Parte opcional sob demanda), especifique o número de unidades sob demanda a serem solicitadas. O número deve ser menor queTotal target capacity (Capacidade total pretendida). O Amazon EC2 calcula e aloca a diferença às unidades spot a serem solicitadas.

Important

Para especificar uma parte sob demanda opcional, primeiro escolha um modelo de execução.

- c. (Opcional) Por padrão, o serviço spot encerra Instâncias spot quando elas são interrompidas. Para manter a capacidade do destino, selecione Maintain target capacity (Manter a capacidade de destino). Em seguida, especifique se as Instâncias spot do serviço Spot são encerradas, paradas ou hibernadas quando forem interrompidas. Para fazer isso, escolha a opção correspondente em Interruption behavior.
- d. (Opcional) Para permitir que a frota spot execute uma instância spot de substituição quando uma notificação de rebalanceamento de instância for emitida para uma instância spot existente na frota, selecione Capacity rebalance (Rebalanceamento de capacidade). Para obter mais informações, consulte [Rebalanceamento de capacidade \(p. 765\)](#).

Note

Quando uma instância de substituição é executada, a instância marcada para rebalanceamento não é automaticamente encerrada. Você pode encerrá-la, ou você pode deixá-la em funcionamento. Você é cobrado por ambas as instâncias enquanto elas estão sendo executadas.

A instância marcada para rebalanceamento tem risco elevado de interrupção e você receberá um aviso de interrupção de dois minutos da Instância spot antes que o Amazon EC2 a interrompa.

- e. (Opcional) Para controlar o valor pago por hora por todas as instâncias spot da sua frota, selecione Manter custo pretendido para instâncias spot e insira o valor total máximo que você está disposto a pagar por hora. Quando o valor total máximo for alcançado, a frota spot interromperá a execução de instâncias spot mesmo que a capacidade do destino ainda não tenha sido atingida. Para obter mais informações, consulte [Controle de gastos \(p. 767\)](#).

7. Em Fleet request settings (Configurações de solicitação de frota), faça o seguinte:

- a. Reveja a solicitação de frota e a estratégia de alocação de frota com base na seleção de sua aplicação ou tarefa. Para alterar os tipos de instância ou a estratégia de alocação, desmarque Apply recommendations (Aplicar recomendações).
- b. (Opcional) Em Fleet allocation strategy (Estratégia de alocação de frota), escolha a estratégia que atende as suas necessidades. Para obter mais informações, consulte [Estratégia de alocação para Instâncias spot \(p. 762\)](#).

- c. (Opcional) Para remover tipos de instância, para Solicitação de frota, selecione os tipos de instância a serem removidos e escolha Excluir. Para adicionar tipos de instância, escolha Select instance types (Selecionar tipos de instância).
8. Em Additional request details (Detalhes de configuração adicionais), faça o seguinte:
 - a. Revise os detalhes de solicitação adicional. Para fazer alterações, desmarque Apply defaults (Aplicar padrões).
 - b. (Opcional) Em IAM fleet role (Função de frota do IAM), você pode usar a função padrão ou especificar uma função diferente. Para usar a função padrão depois de ter alterado a função, escolha Use default role (Usar função padrão).
 - c. (Opcional) Em Maximum price (Preço máximo), você pode usar o preço máximo padrão (preço sob demanda) ou especificar o preço máximo que você está disposto a pagar. Se o seu preço máximo for inferior ao preço spot dos tipos de instâncias selecionados por você, as Instâncias spot não serão executadas.
 - d. (Opcional) Para criar uma solicitação que seja válida somente em um período específico, edite Request valid from e Request valid until.
 - e. (Opcional) Por padrão, encerramos as Instâncias spot quando a solicitação expira. Para mantê-las em execução depois que sua solicitação expirar, desmarque Terminate the instances when the request expires (Encerrar as instâncias na expiração da solicitação).
 - f. (Opcional) Para registrar as Instâncias spot em um load balancer, escolha Receive traffic from one or more load balancers (Receber tráfego de um ou mais load balancers) e escolha um ou mais Classic Load Balancers ou grupos de destino.
9. (Opcional) Para fazer download de uma cópia da configuração de execução para uso com a AWS CLI, escolha JSON config.
10. Escolha Executar.

O tipo de solicitação de frota spot é `fleet`. Quando a solicitação for atendida, as solicitações do tipo `instance` serão adicionadas, onde o estado será `active` e o status será `fulfilled`.

Criar uma frota spot usando a AWS CLI

Para criar uma solicitação de frota spot usando a AWS CLI

- Use o comando `request-spot-fleet` para criar uma solicitação de frota spot.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Para obter arquivos de configuração de exemplo, consulte [Exemplos de configuração de frota spot \(p. 837\)](#).

A seguir está um exemplo de saída:

```
{  
    "SpotFleetRequestId": "sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE"  
}
```

Marcar uma frota spot

Para ajudar a categorizar e gerenciar as solicitações de frota spot, você pode marcá-las com metadados personalizados. Você pode atribuir uma tag a uma solicitação de frota spot ao criá-la ou posteriormente. Você pode atribuir tags usando o console do Amazon EC2 ou uma ferramenta de linha de comando.

Quando você marca uma solicitação de frota spot, as instâncias e os volumes que são executados pela frota spot não são marcados automaticamente. É necessário marcar explicitamente as instâncias e os volumes executados pela frota spot. Você pode optar por atribuir tags somente à solicitação de frota spot, somente às instâncias executadas pela frota, somente aos volumes anexados às instâncias executadas pela frota ou aos todos os três.

Note

As tags de volume são compatíveis apenas para volumes que estão anexados a Instâncias on-demand. Não é possível marcar volumes que estão anexados a Instâncias spot.

Para obter mais informações sobre como as tags funcionam, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

Tópicos

- [Prerequisite \(p. 781\)](#)
- [Marcar uma nova frota spot \(p. 782\)](#)
- [Marcar uma nova frota spot e as instâncias e os volumes que ela executa \(p. 783\)](#)
- [Marcar uma frota spot existente \(p. 785\)](#)
- [Exibir tags de solicitações de frota spot \(p. 786\)](#)

Prerequisite

Conceda ao usuário do IAM permissão para marcar recursos. Para obter mais informações, consulte [Exemplo: marcar recursos \(p. 1178\)](#).

Como conceder a um usuário do IAM permissão para marcar recursos

Crie uma política do IAM que inclua o seguinte:

- A ação `ec2:CreateTags`. Concede ao usuário do IAM permissão para criar tags.
- A ação `ec2:RequestSpotFleet`. Concede ao usuário do IAM permissão para criar uma solicitação de frota spot.
- Para `Resource`, você deve especificar `"*"`. Permite que os usuários marquem todos os tipos de recursos.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "TagSpotFleetRequest",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags",  
                "ec2:RequestSpotFleet"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Important

No momento, não oferecemos suporte para permissões no nível do recurso para o recurso `spot-fleet-request`. Se especificar `spot-fleet-request` como um recurso, você receberá uma exceção não autorizada quando tentar marcar a frota. O exemplo a seguir ilustra como não definir a política.

```
{  
    "Effect": "Allow",  
    "Action": [  
        "ec2:CreateTags",  
        "ec2:RequestSpotFleet"  
    ],  
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"  
}
```

Marcar uma nova frota spot

Como marcar uma nova solicitação de frota spot usando o console

1. Siga o procedimento do [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 777\)](#).
2. Para adicionar uma tag, expanda Additional configurations (Configurações adicionais), escolha Add new tag (Adicionar nova tag) e insira a chave e o valor da tag. Repita esse procedimento para cada tag.

Para cada tag, você pode marcar a solicitação de frota spot e as instâncias com a mesma tag. Para marcar ambas, verifique se Instance tags (Tags de instância) e Fleet tags (Tags de frota) estão selecionados. Para marcar somente a solicitação de frota spot, desmarque Instance tags (Tags de instância). Para marcar apenas as instâncias executadas pela frota, desmarque Fleet tags (Tags de frota).

3. Preencha os campos obrigatórios para criar uma solicitação de frota spot e escolha Launch (Executar). Para obter mais informações, consulte [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 777\)](#).

Como marcar uma nova solicitação de frota spot usando a AWS CLI

Para marcar uma solicitação de frota spot ao criá-la, defina-a da seguinte maneira:

- Especifique as tags para a solicitação de frota spot em SpotFleetRequestConfig.
- Para ResourceType, especifique spot-fleet-request. Se você especificar outro valor, ocorrerá falha na frota.
- Em Tags, especifique o par de chave/valor. Você pode especificar mais de um par de chave/valor.

No exemplo a seguir, a solicitação de frota spot é marcada com duas tags: Key=Environment e Value=Production, e Key=Cost-Center e Value=123.

```
{  
    "SpotFleetRequestConfig": {  
        "AllocationStrategy": "lowestPrice",  
        "ExcessCapacityTerminationPolicy": "default",  
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-role",  
        "LaunchSpecifications": [  
            {  
                "ImageId": "ami-0123456789EXAMPLE",  
                "InstanceType": "c4.large"  
            }  
        ],  
        "SpotPrice": "5",  
        "TargetCapacity": 2,  
        "TerminateInstancesWithExpiration": true,  
        "Type": "maintain",  
        "ReplaceUnhealthyInstances": true,  
        "InstanceInterruptionBehavior": "terminate",  
    }  
}
```

```
"InstancePoolsToUseCount": 1,  
"TagSpecifications": [  
    {  
        "ResourceType": "spot-fleet-request",  
        "Tags": [  
            {  
                "Key": "Environment",  
                "Value": "Production"  
            },  
            {  
                "Key": "Cost-Center",  
                "Value": "123"  
            }  
        ]  
    }  
]
```

Marcar uma nova frota spot e as instâncias e os volumes que ela executa

Como marcar uma nova solicitação de frota spot e as instâncias e os volumes que ela executa usando a AWS CLI

Para marcar uma solicitação de frota spot ao criá-la e marcar as instâncias e os volumes quando elas são executadas pela frota, defina a configuração da solicitação de frota spot da seguinte maneira:

Tags de solicitações de frota spot:

- Especifique as tags para a solicitação de frota spot em `SpotFleetRequestConfig`.
- Para `ResourceType`, especifique `spot-fleet-request`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. Você pode especificar mais de um par de chave/valor.

Tags de instância:

- Especifique as tags das instâncias em `LaunchSpecifications`.
- Para `ResourceType`, especifique `instance`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. Você pode especificar mais de um par de chave/valor.

Como alternativa, você pode especificar as tags da instância no [modelo de execução \(p. 427\)](#) que é referenciado na solicitação de frota spot.

Tags de volume:

- Especifique as tags para os volumes no [modelo de execução \(p. 427\)](#) mencionado na solicitação de frota spot. A marcação de volume em `LaunchSpecifications` não é compatível.

No exemplo a seguir, a solicitação de frota spot é marcada com duas tags: `Key=Environment` e `Value=Production`, e `Key=Cost-Center` e `Value=123`. As instâncias executadas pela frota são marcadas com uma tag (que é a mesma que uma das tags da solicitação de frota spot): `Key=Cost-Center` e `Value=123`.

```
{  
    "SpotFleetRequestConfig": {  
        "AllocationStrategy": "lowestPrice",
```

```
"ExcessCapacityTerminationPolicy": "default",
"IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-role",
"LaunchSpecifications": [
    {
        "ImageId": "ami-0123456789EXAMPLE",
        "InstanceType": "c4.large",
        "TagSpecifications": [
            {
                "ResourceType": "instance",
                "Tags": [
                    {
                        "Key": "Cost-Center",
                        "Value": "123"
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value": "Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value": "123"
                    }
                ]
            }
        ]
    }
}
```

Para marcar instâncias executadas por uma frota spot usando a AWS CLI

Para marcar instâncias quando elas são executadas pela frota, você pode especificar as tags no [modelo de execução \(p. 427\)](#) referenciado na solicitação de frota spot ou especificar as tags na configuração da solicitação de frota spot da seguinte maneira:

- Especifique as tags das instâncias em `LaunchSpecifications`.
- Para `ResourceType`, especifique `instance`. Se você especificar outro valor, ocorrerá falha na frota.
- Em `Tags`, especifique o par de chave/valor. Você pode especificar mais de um par de chave/valor.

No exemplo a seguir, as instâncias que são executadas pela frota são marcadas com uma tag: `Key=Cost-Center` e `Value=123`.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-role",
```

```
"LaunchSpecifications": [
    {
        "ImageId": "ami-0123456789EXAMPLE",
        "InstanceType": "c4.large",
        "TagSpecifications": [
            {
                "ResourceType": "instance",
                "Tags": [
                    {
                        "Key": "Cost-Center",
                        "Value": "123"
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

Para marcar volumes anexados a instâncias sob demanda executadas por uma frota spot usando a AWS CLI

Para marcar volumes ao serem criados pela frota, é necessário especificar as tags no [modelo de execução \(p. 427\)](#) mencionado na solicitação de frota spot.

Note

As tags de volume são compatíveis apenas para volumes que estão anexados a Instâncias on-demand. Não é possível marcar volumes que estão anexados a Instâncias spot.

A marcação de volume em LaunchSpecifications não é compatível.

Marcar uma frota spot existente

Para marcar uma solicitação de frota spot existente usando o console

Depois de criar uma solicitação de frota spot, você pode adicionar tags à solicitação de frota usando o console.

1. Abra o console Spot em <https://console.aws.amazon.com/ec2spot>.
2. Selecione sua solicitação de frota spot.
3. Escolha a guia Tags e Create Tag (Criar tag).

Para marcar uma solicitação de frota spot existente usando a AWS CLI

Você pode usar o comando `create-tags` para marcar os recursos existentes. No exemplo a seguir, a solicitação de frota spot existente é marcada com Key=purpose e Value=test.

```
aws ec2 create-tags \
--resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
--tags Key=purpose,Value=test
```

Exibir tags de solicitações de frota spot

Para exibir tags de solicitação de frota spot usando o console

1. Abra o console Spot em <https://console.aws.amazon.com/ec2spot>.
2. Selecione sua solicitação de frota spot e escolha a guia Tags.

Para descrever as tags de solicitação de frota spot

Use o comando [describe-tags](#) para exibir as tags para o recurso especificado. No exemplo a seguir, você descreve as tags da solicitação de frota spot especificada.

```
aws ec2 describe-tags \
--filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

Você também pode exibir as tags de uma solicitação de frota spot descrevendo a solicitação de frota spot.

Use o comando [describe-spot-fleet-requests](#) para exibir a configuração da solicitação de frota spot especificada, que inclui todas as tags especificadas para a solicitação de frota.

```
aws ec2 describe-spot-fleet-requests \
--spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
            }
        }
    ]
}
```

```
"TargetCapacity": 2,  
"OnDemandTargetCapacity": 0,  
"Type": "maintain",  
"ReplaceUnhealthyInstances": false,  
"InstanceInterruptionBehavior": "terminate"  
},  
"SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",  
"SpotFleetRequestState": "active",  
"Tags": [  
    {  
        "Key": "Environment",  
        "Value": "Production"  
    },  
    {  
        "Key": "Another key",  
        "Value": "Another value"  
    }  
]  
}  
]
```

Monitorar sua frota spot

A frota spot executará instâncias spot quando o preço máximo exceder o preço spot e a capacidade estiver disponível. As Instâncias spot serão executadas até serem interrompidas ou até você as encerrar.

Para monitorar sua frota spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot. Para ver os detalhes da configuração, escolha Description (Descrição).
4. Para listar as instâncias spot para a frota spot, escolha Instances (Instâncias).
5. Para visualizar o histórico da frota spot, escolha a guia History (Histórico).

Para monitorar sua frota spot (AWS CLI)

Use o comando [describe-spot-fleet-requests](#) para descrever as solicitações de frota spot.

```
aws ec2 describe-spot-fleet-requests
```

Use o comando [describe-spot-fleet-instances](#) para descrever as instâncias spot da frota spot especificada.

```
aws ec2 describe-spot-fleet-instances \  
--spot-fleet-request-id sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE
```

Use o comando [describe-spot-fleet-request-history](#) para descrever o histórico da solicitação de frota spot especificada.

```
aws ec2 describe-spot-fleet-request-history \  
--spot-fleet-request-id sfr-73fb2ce-aa30-494c-8788-1cee4EXAMPLE \  
--start-time 2015-05-18T00:00:00Z
```

Modificar uma solicitação de frota spot

Você pode modificar uma solicitação de frota spot ativa para executar as seguintes tarefas:

- Aumentar a capacidade de destino e a porção sob demanda
- Reduzir a capacidade de destino e a porção sob demanda

Note

Você não pode modificar uma solicitação única de frota spot. É possível modificar uma solicitação de frota spot ao selecionar a opção **Maintain target capacity** (Manter capacidade de destino) ao criar a solicitação de frota spot.

Quando você aumenta a capacidade pretendida, a frota spot executa instâncias spot adicionais. Quando você aumenta a parte sob demanda, a frota spot inicia Instâncias sob demanda adicionais.

Quando você aumenta a capacidade pretendida, a frota spot executará as Instâncias spot adicionais de acordo com a estratégia de alocação de solicitação de frota spot. Se a estratégia de alocação for **lowestPrice**, a frota spot executará as instâncias do grupo de capacidade spot que apresentar o menor preço na solicitação de frota spot. Se a estratégia de alocação for **diversified**, a frota spot distribuirá as instâncias pelos grupos na solicitação de frota spot.

Quando você diminui a capacidade de destino, a frota spot cancela todas as solicitações abertas que excedem a nova capacidade pretendida. Você pode solicitar que a frota spot encerre instâncias spot até o tamanho da frota atingir a nova capacidade pretendida. Se a estratégia de alocação for **lowestPrice**, a frota spot encerrará as instâncias com o preço mais alto por unidade. Se a estratégia de alocação for **diversified**, a spot frota encerrará as instâncias nos grupos. Como alternativa, você pode solicitar que a frota spot mantenha seu tamanho atual, mas não substitua as instâncias spot interrompidas ou encerradas manualmente.

Quando uma frota spot encerra uma instância porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

Para modificar uma solicitação de frota spot (console)

1. Abra o console Spot em <https://console.aws.amazon.com/ec2spot/home/fleet>.
2. Selecione sua solicitação de frota spot.
3. Escolha Actions (Ações) e **Modify target capacity** (Modificar capacidade de destino).
4. Em **Modify target capacity** (Modificar capacidade de destino), faça o seguinte:
 - a. Insira a nova capacidade de destino e a porção sob demanda
 - b. (Opcional) Se você estiver reduzindo a capacidade de destino, mas deseja manter a frota no tamanho atual, desmarque **Terminate instances** (Encerrar instâncias).
 - c. Selecione Enviar.

Para modificar uma solicitação de frota spot usando a AWS CLI

Use o comando **modify-spot-fleet-request** para atualizar a capacidade pretendida da solicitação de frota spot especificada.

```
aws ec2 modify-spot-fleet-request \
--spot-fleet-request-id sfr-73fdbd2ce-aa30-494c-8788-1cee4EXAMPLE \
--target-capacity 20
```

Você pode modificar o comando anterior da seguinte forma para diminuir a capacidade de destino da frota spot especificada sem encerrar instâncias spot como resultado.

```
aws ec2 modify-spot-fleet-request \
--spot-fleet-request-id sfr-73fdbd2ce-aa30-494c-8788-1cee4EXAMPLE \
```

```
--target-capacity 10 \
--excess-capacity-termination-policy NoTermination
```

CANCELAR UMA SOLICITAÇÃO DE FROTA SPOT

Ao terminar de utilizar a frota spot, é possível cancelar a solicitação de frota spot. Isso cancelará todas as solicitações spot associadas à frota spot, para que nenhuma instância spot nova seja executada para a frota spot. Você precisa especificar se a frota spot deverá encerrar as respectivas instâncias spot. Se você encerrar as instâncias, a solicitação de frota spot entrará no estado `cancelled_terminating`. Caso contrário, a solicitação de frota spot entrará no estado `cancelled_running` e as instâncias continuarão em execução até que sejam interrompidas ou encerradas manualmente.

Para cancelar uma solicitação de frota spot (console)

1. Abra o console Spot em <https://console.aws.amazon.com/ec2spot/home/fleet>.
2. Selecione sua solicitação de frota spot.
3. Escolha Actions (Ações), Cancel spot request (Cancelar solicitação spot).
4. Em Cancel spot request (Cancelar solicitação spot), certifique-se de que deseja cancelar a frota spot. Para manter a frota no tamanho atual, desmarque Terminate instances (Encerrar instâncias). Quando estiver pronto, escolha Confirmar.

Para cancelar uma solicitação de frota spot usando a AWS CLI

Use o comando `cancel-spot-fleet-requests` para cancelar a solicitação de frota spot especificada e encerrar as instâncias.

```
aws ec2 cancel-spot-fleet-requests \
--spot-fleet-request-ids sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE \
--terminate-instances
```

A seguir está um exemplo de saída:

```
{
  "SuccessfulFleetRequests": [
    {
      "SpotFleetRequestId": "sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE",
      "CurrentSpotFleetRequestState": "cancelled_terminating",
      "PreviousSpotFleetRequestState": "active"
    }
  ],
  "UnsuccessfulFleetRequests": []
}
```

Você pode modificar o comando anterior da seguinte forma para cancelar a solicitação de frota spot especificada sem encerrar as instâncias.

```
aws ec2 cancel-spot-fleet-requests \
--spot-fleet-request-ids sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE \
--no-terminate-instances
```

A seguir está um exemplo de saída:

```
{
  "SuccessfulFleetRequests": [
    {
      "SpotFleetRequestId": "sfr-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE",
      "CurrentSpotFleetRequestState": "cancelled_running",
      "PreviousSpotFleetRequestState": "active"
    }
  ],
  "UnsuccessfulFleetRequests": []
}
```

```
        "CurrentSpotFleetRequestState": "cancelled_running",
        "PreviousSpotFleetRequestState": "active"
    },
    "UnsuccessfulFleetRequests": []
}
```

Métricas do CloudWatch para frota spot

O Amazon EC2 fornece métricas do Amazon CloudWatch que você pode usar para monitorar sua frota spot.

Important

Para garantir uma precisão, recomendamos que você habilite o monitoramento detalhado para usar essas métricas. Para obter mais informações, consulte [Habilitar ou desabilitar monitoramento detalhado para instâncias \(p. 899\)](#).

Para obter mais informações sobre as métricas do CloudWatch fornecidas pelo Amazon EC2, consulte [Monitorar instâncias usando o CloudWatch \(p. 898\)](#).

Métricas de frota spot

O namespace AWS/EC2Spot inclui as métricas a seguir, além das métricas do CloudWatch das Instâncias spot em sua frota. Para obter mais informações, consulte [Métricas de instância \(p. 902\)](#).

Métrica	Descrição
AvailableInstancePoolsCount	Os grupos de capacidade spot especificados na solicitação de frota spot. Unidades: contagem
BidsSubmittedForCapacity	A capacidade para a qual o Amazon EC2 enviou solicitações de frota spot. Unidades: contagem
EligibleInstancePoolCount	Os grupos de capacidade spot especificados na solicitação de frota spot onde o Amazon EC2 pode atender às solicitações. O Amazon EC2 não atende a solicitações em grupos nos quais o preço máximo que você está disposto a pagar por instâncias spot é menor que o preço spot ou o preço spot é maior que o preço das instâncias sob demanda. Unidades: contagem
FulfilledCapacity	A capacidade preenchida pelo Amazon EC2. Unidades: contagem
MaxPercentCapacityAllocation	O valor máximo de PercentCapacityAllocation em todos os grupos de frota spot especificados na solicitação de frota spot. Unidades: percentual
PendingCapacity	A diferença entre TargetCapacity e FulfilledCapacity. Unidades: contagem

Métrica	Descrição
PercentCapacityAllocation	A capacidade alocada para o grupo de capacidade spot para as dimensões especificadas. Para obter o valor máximo registrado em todos os grupos de capacidade spot, use MaxPercentCapacityAllocation. Unidades: percentual
TargetCapacity	A capacidade pretendida da solicitação de frota spot. Unidades: contagem
TerminatingCapacity	A capacidade que está sendo encerrada, pois a capacidade provisionada é maior que a capacidade de destino. Unidades: contagem

Se a unidade de medida para uma métrica é Count, a estatística mais útil é Average.

Dimensões da frota spot

Para filtrar os dados da frota spot, use as dimensões a seguir.

Dimensões	Descrição
AvailabilityZone	Filtre os dados por zona de disponibilidade.
FleetRequestId	Filtre os dados por solicitação de frota de spot.
InstanceType	Filtre os dados por tipo de instância.

Exibir as métricas do CloudWatch para sua frota spot

Você pode exibir as métricas do CloudWatch para sua frota spot usando o console do Amazon CloudWatch. Essas métricas são exibidas como gráficos de monitoramento. Esses gráficos mostrarão pontos de dados se a frota spot estiver ativa.

As métricas são agrupadas primeiro pelo namespace e, em seguida, por várias combinações de dimensões dentro de cada namespace. Por exemplo, você pode exibir todas as métricas da frota spot ou grupos de métricas de frota spot por ID de solicitação de frota spot, tipo de instância ou Zona de disponibilidade.

Para exibir métricas de frota spot

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace do EC2 Spot.

Note

Se o namespace do EC2 Spot não for exibido, há dois motivos para isso. Você ainda não usou a frota spot, apenas os produtos da AWS em uso enviam métricas para o Amazon CloudWatch. Ou, se você não tiver usado a frota spot nas últimas duas semanas, o namespace não será exibido.

4. (Opcional) Para filtrar as métricas por dimensão, selecione uma das seguintes ações:
 - Fleet Request Metrics (Métricas de solicitação da frota): agrupar por solicitação de frota spot
 - By Availability Zone (Por zona de disponibilidade): agrupar por solicitação de frota spot e zona de disponibilidade
 - By Instance Type (Por tipo de instância): agrupar por solicitação de frota spot e tipo de instância
 - By Availability Zone/Instance Type (Por zona de disponibilidade/tipo de instância): agrupar por solicitação de frota spot, zona de disponibilidade e tipo de instância
5. Para visualizar os dados de uma métrica, marque a caixa de seleção ao lado da métrica.

FleetRequestId	Metric Name
sfr-4a707781-8fac-459b-a5ae-4701fcee47d7	AvailableInstancePoolsCount
sfr-4a707781-8fac-459b-a5ae-4701fcee47d7	BidsSubmittedForCapacity
<input checked="" type="checkbox"/> sfr-4a707781-8fac-459b-a5ae-4701fcee47d7	CPUUtilization
sfr-4a707781-8fac-459b-a5ae-4701fcee47d7	DiskReadBytes

Escalabilidade automática para frota spot

A escalabilidade automática é a capacidade de aumentar ou diminuir a capacidade de destino de sua frota spot automaticamente com base na demanda. Uma frota spot pode executar instâncias (aumentar a escala na horizontal) ou encerrar instâncias (reduzir a escala na horizontal), no intervalo escolhido, em resposta a uma ou mais políticas de escalabilidade.

A frota spot oferece suporte aos seguintes tipos de escalabilidade automática:

- [Escalabilidade do monitoramento do objetivo \(p. 794\)](#): aumenta ou diminui a capacidade atual da frota com base em um valor pretendido para uma métrica específica. Isso é semelhante à forma como o termostato mantém a temperatura da sua casa, ou seja, você seleciona a temperatura e o termostato faz o resto.
- [Escalabilidade em etapas \(p. 795\)](#): aumenta ou diminui a capacidade atual da frota com base em um conjunto de ajustes de escalabilidade, conhecidos como ajustes em etapas, que variam com base no tamanho da ruptura do alarme.
- [Escalabilidade programado \(p. 797\)](#): aumenta ou diminui a capacidade atual da frota com base em data e hora.

Se estiver usando [peso da instância \(p. 768\)](#), lembre-se de que a frota spot pode exceder a capacidade de destino conforme necessário. A capacidade atendida pode ser um número de ponto flutuante, mas a capacidade de destino deve ser um inteiro, portanto, a frota spot é arredondada para o próximo inteiro. Você deve levar em conta esses comportamentos ao ver o resultado de uma política de escalabilidade quando um alarme é acionado. Por exemplo, suponha que a capacidade de destino seja 30, a capacidade atendida seja 30,1 e a política de escalabilidade subtraia 1. Quando o alarme é acionado, o processo de escalabilidade automática subtrairá 1 de 30,1 para obter 29,1 e o arredondará para 30, portanto, nenhuma ação de escalabilidade é executada. Suponhamos também que você selecione os pesos de instância 2, 4 e 8 e uma capacidade de destino igual a 10, mas nenhuma instância de peso 2 esteja disponível. Sendo

assim, a frota spot provisionou instâncias de pesos 4 e 8 para uma capacidade atendida igual a 12. Se a política de escalabilidade reduzir a capacidade de destino em 20% e um alarme for acionado, o processo de escalabilidade automática subtrairá $12 \times 0,2$ de 12 para obter 9,6 e o arredondará para 10, portanto, nenhuma ação de escalabilidade será executada.

As políticas de escalabilidade que podem ser criadas para a frota spot oferecem suporte a um período de desaquecimento. Esse é o número de segundos após o encerramento de uma ação de escalabilidade em que as atividades de escalabilidade anteriores, relacionadas ao acionamento, podem influenciar eventos futuros de escalabilidade. Para expandir as políticas enquanto o período do desaquecimento estiver em vigor, a capacidade que foi adicionada pelo evento de expansão anterior que iniciou o desaquecimento é calculada como parte da capacidade desejada para a expansão seguinte. A intenção é expandir de forma contínua (mas não excessivamente). Para políticas de redução, o período do desaquecimento é utilizado para bloquear a escala subsequente nas solicitações até que expire. A intenção é reduzir de forma conservadora para proteger a disponibilidade de sua aplicação. Contudo, se outro alarme acionar uma política de expansão durante o período do desaquecimento após uma redução, a escalabilidade automática expandirá seu destino dimensionável imediatamente.

Recomendamos que você defina a escalabilidade com base nas métricas da instância com intervalos de 1 minuto, pois isso garante resposta mais rápida às mudanças de utilização. Aumentar a escalabilidade com base em métricas com intervalos de cinco minutos pode resultar em tempo de resposta mais lento e na escalabilidade com base em dados de métricas obsoletos. Para enviar dados de métrica das instâncias ao CloudWatch em períodos de 1 minuto, você deve habilitar especificamente o monitoramento detalhado. Para obter mais informações, consulte [Habilitar ou desabilitar o monitoramento detalhado para instâncias \(p. 899\)](#) e [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 777\)](#).

Para obter mais informações sobre configuração de escalabilidade para a frota spot, consulte os recursos a seguir:

- Seção [application-autoscaling](#) da AWS CLI Command Reference (Referência de comandos da AWS CLI).
- [Referência à API do Application Auto Scaling](#)
- [Guia do usuário do Application Auto Scaling](#)

Permissões do IAM obrigatórias para escalabilidade automática de frota spot

A escalabilidade automática para frota spot é possível por uma combinação das APIs do Amazon EC2, do Amazon CloudWatch e do Application Auto Scaling. As solicitações de frota spot são criadas com o Amazon EC2, os alarmes são criados com o CloudWatch e as políticas de escalabilidade são criadas com o Application Auto Scaling.

Além das [permissões do IAM para a frota spot \(p. 772\)](#) e Amazon EC2, o usuário do IAM que acessa as configurações de escala de frota deve ter as permissões adequadas para os serviços que ofereçam suporte à escalabilidade dinâmica. Os usuários do IAM precisam ter as permissões para usar as ações mostradas na política de exemplo a seguir.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "application-autoscaling:*",  
                "ec2:DescribeSpotFleetRequests",  
                "ec2:ModifySpotFleetRequest",  
                "cloudwatch:DeleteAlarms",  
                "cloudwatch:PutMetricAlarm",  
                "cloudwatch:PutMetricData"  
            ]  
        }  
    ]  
}
```

```
    "cloudwatch:DescribeAlarmHistory",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "cloudwatch:GetMetricStatistics",
    "cloudwatch>ListMetrics",
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DisableAlarmActions",
    "cloudwatch:EnableAlarmActions",
    "iam>CreateServiceLinkedRole",
    "sns>CreateTopic",
    "sns:Subscribe",
    "sns:Get*",
    "sns>List*"
],
"Resource": "*"
}
]
```

Também é possível criar suas próprias políticas do IAM que permitem permissões mais refinadas para chamadas à API do Application Auto Scaling. Para obter mais informações, consulte [Controle de acesso e autenticação](#) no Manual do usuário do Application Auto Scaling.

O serviço do Application Auto Scaling também precisa de permissão para descrever a frota spot e os alarmes do CloudWatch, além de permissões para modificar a capacidade de destino da frota spot em seu nome. Se você habilitar a escalabilidade automática para a frota spot, ela criará uma função vinculada ao serviço chamada `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest`. Essa função vinculada ao serviço concede ao Application Auto Scaling permissão para descrever os alarmes das políticas, monitorar a capacidade atual da frota e modificar a capacidade da frota. A função de frota spot gerenciada original para o Application Auto Scaling era `aws-ec2-spot-fleet-autoscale-role`, mas ela não é mais necessária. Essa função vinculada ao serviço é a função padrão do Application Auto Scaling. Para obter mais informações, consulte [Funções vinculadas ao serviço](#) no Manual do usuário do Application Auto Scaling.

Alterar a escala da frota spot usando as políticas de monitoramento do objetivo

Com as políticas de dimensionamento com monitoramento do objetivo, você seleciona uma métrica e define um valor pretendido. A frota spot cria e gerencia os alarmes do CloudWatch que acionam a política de escalabilidade e calculam o ajuste de escalabilidade com base na métrica e no valor de destino. A política de escalabilidade adiciona ou remove capacidade conforme necessário para manter a métrica no valor de destino especificado ou próxima a ele. Além de manter a métrica próxima ao valor de destino, uma política de escalabilidade de rastreamento de destino também se ajusta às flutuações na métrica, devido a um padrão de carga de flutuação, e minimiza as flutuações rápidas na capacidade da frota.

Você pode criar várias políticas de dimensionamento com monitoramento do objetivo para uma frota spot, desde que cada uma delas use uma métrica diferente. A escalabilidade da frota se baseia na política que fornece a maior capacidade da frota. Com isso, é possível cobrir vários cenários e garantir que sempre haja capacidade suficiente para processar suas workloads de aplicações.

Para garantir a disponibilidade da aplicação, a frota se expande proporcionalmente à métrica o mais rápido possível, mas se retrai gradualmente.

Quando uma frota spot encerra uma instância porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

Não edite ou exclua os alarmes do CloudWatch que a frota spot gerencia para uma política de dimensionamento com monitoramento do objetivo. A frota spot exclui os alarmes automaticamente quando você exclui a política de dimensionamento com monitoramento do objetivo.

Limitation

A solicitação de frota spot deve ter o tipo de solicitação `maintain`. A escalabilidade automática não é compatível com solicitações do tipo `request` nem blocos spot.

Para configurar uma política de rastreamento (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione a solicitação de frota spot e escolha Auto Scaling.
4. Se a escalabilidade automática não estiver configurada, escolha Configurar.
5. Use Escalar capacidade entre para definir a capacidade mínima e máxima para sua frota. A escalabilidade automática não dimensiona a frota abaixo da capacidade mínima ou acima da capacidade máxima.
6. Em Policy Name (Nome da política), digite um nome para a política.
7. Escolha uma Target metric.
8. Digite um Target value (Valor de destino) para a métrica.
9. (Opcional) Defina Cooldown period para modificar o desaquecimento padrão.
10. (Opcional) Selecione Disable scale-in para omitir a criação de uma política de redução baseada na configuração atual. Você pode criar uma política de redução usando uma configuração diferente.
11. Escolha Save (Salvar).

Para configurar uma política de rastreamento de destino usando a AWS CLI

1. Registre a solicitação de frota spot como um destino escalável usando o comando [register-scalable-target](#).
2. Crie uma política de escalabilidade usando o comando [put-scaling-policy](#).

Alterar a escala da frota spot usando políticas de escalabilidade em etapas

Com as políticas de escalabilidade em etapas, você especifica os alarmes do CloudWatch para acionamento do processo de escalabilidade. Por exemplo, se você deseja aumentar a escala quando a utilização de CPU atinge um determinado nível, crie um alarme usando a métrica `CPUUtilization` fornecida pelo Amazon EC2.

Ao criar uma política de escalabilidade em etapas, você deve especificar um dos seguintes tipos de ajuste de escalabilidade:

- Add (Adicionar): aumente a capacidade de destino da frota por um número específico de unidades de capacidade ou por uma porcentagem especificada da capacidade atual.
- Remove (Remover): reduza a capacidade de destino da frota por um número específico de unidades de capacidade ou por uma porcentagem especificada da capacidade atual.
- Set to (Definir como): defina a capacidade de destino da frota como o número especificado de unidades de capacidade.

Quando um alarme é acionado, o processo de escalabilidade automática calcula a nova capacidade de destino usando a capacidade atendida e as políticas de escalabilidade e, em seguida, atualiza a capacidade de destino corretamente. Por exemplo, suponha que a capacidade de destino e a capacidade atendida sejam 10 e a política de escalabilidade seja 1. Quando o alarme é acionado, o processo de escalabilidade automática adiciona 1 a 10 para obter 11, para que a frota execute uma instância.

Quando uma frota spot encerra uma instância porque a capacidade pretendida foi diminuída, a instância recebe um aviso de interrupção de instância spot.

Limitation

A solicitação de frota spot deve ter o tipo de solicitação `maintain`. A escalabilidade automática não é compatível com solicitações do tipo `request` nem blocos spot.

Prerequisites

- Considere quais métricas do CloudWatch são importantes para sua aplicação. Você pode criar alarmes do CloudWatch com base nas métricas fornecidas pela AWS ou suas próprias métricas personalizadas.
- Para as métricas da AWS que você usará em suas políticas de escalabilidade, habilite a coleta de CloudWatch métricas se o serviço que fornece as métricas não as habilitar por padrão.

Criar um alarme do CloudWatch

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Alarms.
3. Selecione Create alarm (Criar alarme).
4. Na página Specify metric and conditions (Especificar métrica e condições), selecione Select metric (Selecionar métrica).
5. Escolha Spot do EC2, Métricas de solicitação de frota, selecione uma métrica (por exemplo, TargetCapacity) e escolha Selecionar métrica.

A página Specify metric and conditions (Especificar métrica e condições) será exibida, mostrando um gráfico e outras informações sobre a métrica selecionada.

6. Em Period (Período), escolha o período de avaliação para o alarme, por exemplo, 1 minuto. Ao avaliar o alarme, todos os períodos são agregados em um único ponto de dados.

Note

Um período mais curto cria um alarme mais sensível.

7. Em Conditions (Condições), defina o alarme definindo a condição do limite. Por exemplo, é possível definir um limite para acionar o alarme sempre que o valor da métrica for maior que ou igual a 80%.
8. Em Additional configuration (Configuração adicional), para Datapoints to alarm (Pontos de dados para alarme), especifique quantos pontos de dados (períodos de avaliação) devem estar no estado ALARM para acionar o alarme, por exemplo, 1 período de avaliação para 2 de 3 períodos de avaliação. Isso cria um alarme que passará para o estado ALARM se houver violação de muitos períodos consecutivos. Para obter mais informações, consulte [Como avaliar um alarme](#) em Guia do usuário do Amazon CloudWatch.
9. Para Missing data treatment (Tratamento de dados ausentes), selecione uma das opções (ou mantenha o padrão como Treat missing data as missing (Tratar dados ausentes como ausentes)). Para obter mais informações, consulte [Configuração da forma como os alarmes do CloudWatch tratam dados ausentes](#) no Guia do usuário do Amazon CloudWatch.
10. Escolha Next (Próximo).
11. (Opcional) Para receber notificações de um evento de dimensionamento, para Notification (Notificação), é possível escolher ou criar o tópico do Amazon SNS que você deseja usar para receber notificações. Caso contrário, você poderá excluir a notificação agora e adicionar uma posteriormente, quando necessário.
12. Escolha Next (Próximo).
13. Em Add a description (Adicionar uma descrição), insira um nome e uma descrição para o alarme e selecione Next (Próximo).
14. Selecione Create alarm (Criar alarme).

Para configurar uma política de escalabilidade para a frota spot (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione a solicitação de frota spot e escolha Auto Scaling.
4. Se a escalabilidade automática não estiver configurada, escolha Configurar.
5. Use Escalar capacidade entre para definir a capacidade mínima e máxima para sua frota. A escalabilidade automática não dimensiona a frota abaixo da capacidade mínima ou acima da capacidade máxima.
6. Inicialmente, a opção Políticas de escalabilidade contém as políticas denominadas ScaleUp e ScaleDown. Você pode completar essas políticas ou escolher Remover política para excluí-las. Você também pode escolher Add policy (Adicionar política).
7. Para definir a política, faça o seguinte:
 - a. Em Policy Name (Nome da política), digite um nome para a política.
 - b. Em Policy trigger (Gatilho de políticas), selecione um alarme existente ou escolha Create new alarm (Criar novo alarme) para abrir o console do Amazon CloudWatch e criar um alarme.
 - c. Em Modificar capacidade, selecione um tipo de ajuste de escalabilidade, um número e uma unidade.
 - d. (Opcional) Para executar a escalabilidade em etapas, escolha Definir etapas. Por padrão, uma política de adição tem um limite de -infinitude menor e um limite superior do limite de alarme. Por padrão, uma política de remoção tem um limite menor do limite de alarme e um limite maior de +infinitude. Para adicionar outra etapa, escolha Adicionar etapa.
 - e. (Opcional) Para modificar o valor padrão para o período do desaquecimento, selecione um número em Período de desaquecimento.
8. Escolha Save (Salvar).

Para configurar políticas de escalabilidade em etapas para sua frota spot usando a AWS CLI

1. Registre a solicitação de frota spot como um destino escalável usando o comando `register-scaling-target`.
2. Crie uma política de escalabilidade usando o comando `put-scaling-policy`.
3. Crie um alarme que acione as políticas de escalabilidade usando o comando `put-metric-alarm`.

Alterar a escala da frota spot usando a escalabilidade programada

A escalabilidade com base em uma programação permite que você dimensione sua aplicação em resposta a alterações de demanda. Para usar a escalabilidade programada, crie ações programadas que instruam a frota spot a executar ações de escalabilidade em momentos específicos. Ao criar uma ação programada, você especifica uma frota spot existente, quando a ação de escalabilidade deve ocorrer, a capacidade mínima e a capacidade máxima. É possível criar ações programadas para escalar uma única vez ou de forma programada.

Você só pode criar uma ação programada para Frotas spot que já existe. Não é possível criar uma ação programada ao mesmo tempo em que você cria uma frota spot.

Limitation

A solicitação de frota spot deve ter o tipo de solicitação `maintain`. A escalabilidade automática não é compatível com solicitações do tipo `request` nem blocos spot.

Para criar uma única ação programada

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e a guia Scheduled Scaling (Escalabilidade programada) próximo à parte inferior da tela.
4. Escolha Create Scheduled Action (Criar ação programada).
5. Em Name (Nome), especifique um nome para a ação programada.
6. Insira um valor para Minimum capacity (Capacidade mínima), Maximum capacity (Capacidade máxima), ou ambos.
7. Em Recurrence (Recorrência), escolha Once (Uma vez).
8. (Opcional) Escolha uma data e hora para Start time (Hora de início), End time (Hora de término), ou ambos.
9. Selecione Enviar.

Para escalar em uma programação recorrente

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e a guia Scheduled Scaling (Escalabilidade programada) próximo à parte inferior da tela.
4. Em Recurrence (Recorrência), escolha uma das programações predefinidas (por exemplo, Every day (Todos os dias)) ou escolha Custom (Personalizado) e digite uma expressão cron. Para obter mais informações sobre as expressões cron compatíveis com a escalabilidade programada, consulte [Expressões cron](#) no Guia do usuário do Amazon CloudWatch Events.
5. (Opcional) Escolha uma data e hora para Start time (Hora de início), End time (Hora de término), ou ambos.
6. Selecione Enviar.

Para editar uma ação programada

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e a guia Scheduled Scaling (Escalabilidade programada) próximo à parte inferior da tela.
4. Selecione a ação programada e escolha Actions (Ações), Edit (Editar).
5. Faça as alterações necessárias e escolha Submit (Enviar).

Para excluir uma ação programada

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Solicitações spot.
3. Selecione sua solicitação de frota spot e a guia Scheduled Scaling (Escalabilidade programada) próximo à parte inferior da tela.
4. Selecione a ação programada e escolha Actions (Ações), Delete (Excluir).
5. Quando a confirmação for solicitada, escolha Excluir.

Para gerenciar a escalabilidade programada usando o AWS CLI

Use os seguintes comandos:

- [put-scheduled-action](#)
- [describe-scheduled-actions](#)
- [delete-scheduled-action](#)

Monitorar eventos da frota usando o Amazon EventBridge

Quando o estado de uma Frota do EC2 é alterado, a Frota do EC2 emite uma notificação. A notificação é disponibilizada como um evento que é enviado para Amazon EventBridge (anteriormente conhecido como Amazon CloudWatch Events). Eventos são emitidos com base no melhor esforço.

Com Amazon EventBridge, você pode criar regras que açãoam ações programáticas em resposta a um evento. Por exemplo, você pode criar duas regras de EventBridge, uma que é açãoada quando um estado da frota muda e uma que é açãoada quando uma instância na frota é encerrada. Se o estado da frota for alterado, a primeira regra invocará um tópico do SNS para enviar uma notificação por e-mail para você. Se uma instância for encerrada, a segunda regra de invocará uma função do Lambda para executar uma nova instância.

Tópicos

- [Tipos de evento de Frota do EC2 \(p. 799\)](#)
- [Tipos de evento de frota spot \(p. 803\)](#)
- [Criar uma regra do Amazon EventBridge \(p. 808\)](#)

Tipos de evento de Frota do EC2

Note

Apenas frotas do tipo `maintain` e `request` emitem eventos. As frotas do tipo `instant` não emitem eventos porque enviam solicitações únicas síncronas e o estado da frota é conhecido imediatamente na resposta.

Existem cinco tipos de eventos de Frota do EC2. Para cada tipo de evento, existem vários subtipos.

Os eventos são enviados para EventBridge no formato JSON. Os seguintes campos no evento formam o padrão de evento definido na regra e que açãoam uma ação:

```
"source": "aws.ec2fleet"  
  
        Identifica que o evento é de Frota do EC2.  
"detail-type": "EC2 Fleet State Change"  
  
        Identifica o tipo de evento.  
"detail": { "sub-type": "submitted" }  
  
        Identifica o subtipo de evento.
```

Tipos de evento

- [Alteração do estado da EC2 Fleet \(p. 800\)](#)
- [Alteração da solicitação de instância spot da EC2 Fleet \(p. 801\)](#)
- [Alteração da instância da EC2 Fleet \(p. 801\)](#)
- [Informações da EC2 Fleet \(p. 802\)](#)
- [Erro de EC2 Fleet \(p. 803\)](#)

Alteração do estado da EC2 Fleet

A Frota do EC2 envia um evento `EC2 Fleet State Change` para Amazon EventBridge quando um estado Frota do EC2 mudar.

A seguir estão dados de exemplo para esse evento.

```
{  
    "version": "0",  
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",  
    "detail-type": "EC2 Fleet State Change",  
    "source": "aws.ec2fleet",  
    "account": "123456789012",  
    "time": "2020-11-09T09:00:20Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-be4d-6b0809bfff0a"  
    ],  
    "detail": {  
        "sub-type": "active"  
    }  
}
```

Os possíveis valores para `sub-type` são:

`submitted`

A solicitação de Frota do EC2 está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de destino de instâncias.

`active`

A solicitação de Frota do EC2 foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias spot.

`progress`

A solicitação de Frota do EC2 está em processo de ser atendida.

`cancelled_terminating`

A solicitação de Frota do EC2 foi excluída, e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

`cancelled_running`

A solicitação de Frota do EC2 foi excluída e não executará instâncias adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas.

`cancelled`

A solicitação de Frota do EC2 foi excluída, e não há outras instâncias em execução. A solicitação de Frota do EC2 foi excluída dois dias depois que as instâncias foram encerradas.

`modify_in_progress`

A solicitação de Frota do EC2 está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada ou que a solicitação de Frota do EC2 seja excluída.

`modify_succeeded`

A solicitação de Frota do EC2 foi modificada. Este estado não se aplica às frotas de `instant` porque as frotas de `instant` não podem ser modificadas.

expired

A solicitação de Frota do EC2 expirou. Se a solicitação tiver sido criada com conjunto de `TerminateInstancesWithExpiration`, um evento subsequente indicará que as instâncias estão encerradas.

Alteração da solicitação de instância spot da EC2 Fleet

A Frota do EC2 envia um evento de `EC2 Fleet Spot Instance Request Change` para Amazon EventBridge quando uma solicitação de Instância spot na frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{  
    "version": "0",  
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",  
    "detail-type": "EC2 Fleet Spot Instance Request Change",  
    "source": "aws.ec2fleet",  
    "account": "123456789012",  
    "time": "2020-11-09T09:00:05Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:123456789012:fleet/  
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"  
    ],  
    "detail": {  
        "spot-instance-request-id": "sir-rmqsk6h",  
        "description": "SpotInstanceRequestId sir-rmqsk6h, PreviousState:  
cancelled_running",  
        "sub-type": "cancelled"  
    }  
}
```

Os possíveis valores para `sub-type` são:

submitted

A solicitação é enviada.

disabled

Você interrompeu a Instância spot.

active

A solicitação foi atendida e tem uma instância spot associada.

cancelled

Você cancelou a solicitação ou ela expirou.

Alteração da instância da EC2 Fleet

O Frota do EC2 envia um evento de `EC2 Fleet Instance Change` para Amazon EventBridge quando uma instância na frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{  
    "version": "0",  
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",  
    "detail-type": "EC2 Fleet Instance Change",  
    "source": "aws.ec2fleet",  
    "account": "123456789012",  
    "time": "2020-11-09T09:00:05Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:123456789012:fleet/  
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"  
    ],  
    "detail": {  
        "instance-id": "i-00000000000000000",  
        "state": "terminated",  
        "status": "terminated",  
        "previous-state": "running",  
        "sub-type": "terminated"  
    }  
}
```

```
"source": "aws.ec2fleet",
"account": "123456789012",
"time": "2020-11-09T09:00:23Z",
"region": "us-east-1",
"resources": [
    "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
],
"detail": {
    "instance-id": "i-0c594155dd5ff1829",
    "description": "{\"instanceType\":\"c5.large\", \"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\", \"availabilityZone\":\"us-east-1d\"}",
    "sub-type": "launched"
}
}
```

Os possíveis valores para sub-type são:

launched

Uma nova instância foi executada.

terminated

A instância foi encerrada.

termination_notified

Uma notificação de encerramento de instância foi enviada.

Informações da EC2 Fleet

A Frota do EC2 envia um evento de EC2 Fleet Information para Amazon EventBridge quando há um erro durante a execução. O evento informativo não impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot bid
price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
}
```

Os possíveis valores para sub-type são:

launchSpecUnusable

O preço em uma especificação de execução não é válido porque está abaixo do preço spot ou o preço spot está acima do preço sob demanda.

fleetProgressHalted

O preço em cada especificação de execução não é válido. Uma especificação de execução pode se tornar válida se o preço spot mudar.

registerWithLoadBalancersFailed

Falha na tentativa de registrar instâncias com平衡adores de carga. Para obter mais informações, consulte a descrição do evento.

launchSpecTemporarilyBlacklisted

A configuração não é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

Erro de EC2 Fleet

A Frota do EC2 envia um evento de `EC2 Fleet Error` para Amazon EventBridge quando há um erro durante a execução. O evento de erro impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{  
    "version": "0",  
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",  
    "detail-type": "EC2 Fleet Error",  
    "source": "aws.ec2fleet",  
    "account": "123456789012",  
    "time": "2020-10-07T01:44:24Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-  
d33e68eafa08"  
    ],  
    "detail": {  
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not supported  
for the instance type 'm3.large'. ",  
        "sub-type": "spotFleetRequestConfigurationInvalid"  
    }  
}
```

Os possíveis valores para `sub-type` são:

allLaunchSpecsTemporarilyBlacklisted

Nenhuma das configurações é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

spotFleetRequestConfigurationInvalid

A configuração não é válida. Para obter mais informações, consulte a descrição do evento.

spotInstanceCountLimitExceeded

Você atingiu o limite do número de Instâncias spot que você pode executar.

Tipos de evento de frota spot

Existem cinco tipos de eventos de frota spot. Para cada tipo de evento, existem vários subtipos.

Os eventos são enviados para EventBridge no formato JSON. Os seguintes campos no evento formam o padrão de evento definido na regra e que acionam uma ação:

```
"source": "aws.ec2spotfleet"  
  
Identifica que o evento é da frota spot.  
"detail-type": "EC2 Spot Fleet State Change"  
  
Identifica o tipo de evento.  
"detail": { "sub-type": "submitted" }  
  
Identifica o subtipo de evento.
```

Tipos de evento

- [Alteração do estado da frota spot do EC2 \(p. 804\)](#)
- [Alteração da solicitação de instância spot da frota spot do EC2 \(p. 805\)](#)
- [Alteração da instância da frota spot do EC2 \(p. 806\)](#)
- [Informações sobre a frota spot do EC2 \(p. 806\)](#)
- [Erro na frota spot do EC2 \(p. 807\)](#)

Alteração do estado da frota spot do EC2

A Frota spot envia um `EC2 Spot Fleet State Change` evento para Amazon EventBridge quando uma frota spot muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{  
    "version": "0",  
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",  
    "detail-type": "EC2 Spot Fleet State Change",  
    "source": "aws.ec2spotfleet",  
    "account": "123456789012",  
    "time": "2020-11-09T08:57:06Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-  
        b3be-9dc627ad1f55"  
    ],  
    "detail": {  
        "sub-type": "submitted"  
    }  
}
```

Os possíveis valores para `sub-type` são:

`submitted`

A solicitação de frota spot está sendo avaliada, e o Amazon EC2 está se preparando para executar o número de destino de instâncias.

`active`

A solicitação de frota spot foi validada e o Amazon EC2 está tentando manter o número de destino das instâncias spot em execução.

`progress`

A solicitação de frota spot está em processo de atendimento.

cancelled_terminating

A solicitação de frota spot é excluída, e as instâncias estão sendo encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam encerradas.

cancelled_running

A solicitação de frota spot é excluída e não executa instâncias adicionais. Suas instâncias existentes continuam sendo executadas até que sejam interrompidas ou encerradas. A solicitação permanece nesse estado até que todas as instâncias sejam interrompidas ou encerradas.

cancelled

A solicitação de frota spot é excluída e não tem instâncias em execução. A frota spot será excluída dois dias após o encerramento das instâncias.

modify_in_progress

A solicitação de frota spot está sendo modificada. A solicitação permanece nesse estado até que a modificação seja totalmente processada ou que a solicitação de frota spot seja excluída.

modify_succeeded

A solicitação de frota spot foi modificada.

expired

A solicitação de frota spot expirou. Se a solicitação tiver sido criada com conjunto de `TerminateInstancesWithExpiration`, um evento subsequente indicará que as instâncias estão encerradas.

Alteração da solicitação de instância spot da frota spot do EC2

A Frota spot envia um evento de `EC2_Spot_Fleet_Spot_Instance_Request_Change` para Amazon EventBridge quando uma solicitação de Instância spot da frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{  
    "version": "0",  
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",  
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",  
    "source": "aws.ec2spotfleet",  
    "account": "123456789012",  
    "time": "2020-11-09T08:53:21Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request:sfr-  
a98d2133-941a-47dc-8b03-0f94c6852ad1"  
    ],  
    "detail": {  
        "spot-instance-request-id": "sir-a2w9gc5h",  
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:  
cancelled_running",  
        "sub-type": "cancelled"  
    }  
}
```

Os possíveis valores para `sub-type` são:

submitted

A solicitação é enviada.

disabled

Você interrompeu a Instância spot.

active

A solicitação foi atendida e tem uma instância spot associada.

cancelled

Você cancelou a solicitação ou ela expirou.

Alteração da instância da frota spot do EC2

A frota spot envia um evento de `EC2 Spot Fleet Instance Change` para Amazon EventBridge quando uma instância na frota muda de estado.

A seguir estão dados de exemplo para esse evento.

```
{  
    "version": "0",  
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",  
    "detail-type": "EC2 Spot Fleet Instance Change",  
    "source": "aws.ec2spotfleet",  
    "account": "123456789012",  
    "time": "2020-11-09T07:25:02Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-  
af9c-0095e6e3ba61"  
    ],  
    "detail": {  
        "instance-id": "i-08b90df1e09c30c9b",  
        "description": "{\"instanceType\":\"r4.2xlarge\", \"image\":\"ami-032930428bf1abbff\", \"productDescription\":\"Linux/UNIX\", \"availabilityZone\":\"us-east-1a\"}",  
        "sub-type": "launched"  
    }  
}
```

Os possíveis valores para `sub-type` são:

launched

Uma nova instância foi executada.

terminated

A instância foi encerrada.

termination_notified

Uma notificação de encerramento de instância foi enviada.

Informações sobre a frota spot do EC2

A frota spot envia um evento de `EC2 Spot Fleet Information` para Amazon EventBridge quando há um erro durante o atendimento. O evento informativo não impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
```

```
"version": "0",
"id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
"detail-type": "EC2 Spot Fleet Information",
"source": "aws.ec2spotfleet",
"account": "123456789012",
"time": "2020-11-08T20:56:12Z",
"region": "us-east-1",
"resources": [
    "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
],
"detail": {
    "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot bid
price is less than Spot market price $0.5291",
    "sub-type": "launchSpecUnusable"
}
}
```

Os possíveis valores para sub-type são:

launchSpecUnusable

O preço em uma especificação de execução não é válido porque está abaixo do preço spot ou o preço spot está acima do preço sob demanda.

fleetProgressHalted

O preço em cada especificação de execução não é válido. Uma especificação de execução pode se tornar válida se o preço spot mudar.

registerWithLoadBalancersFailed

Falha na tentativa de registrar instâncias com平衡adores de carga. Para obter mais informações, consulte a descrição do evento.

launchSpecTemporarilyBlacklisted

A configuração não é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

Erro na frota spot do EC2

A frota spot envia um evento do **EC2 Spot Fleet Error** para Amazon EventBridge quando há um erro durante o atendimento. O evento de erro impede a frota de tentar atender à sua capacidade de destino.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
associatePublicIPAddress parameter can only be specified for the network interface with
DeviceIndex 0. "
    }
}
```

```
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
```

Os possíveis valores para `sub-type` são:

`allLaunchSpecsTemporarilyBlacklisted`

Nenhuma das configurações é válida e várias tentativas de executar instâncias falharam. Para obter mais informações, consulte a descrição do evento.

`spotFleetRequestConfigurationInvalid`

A configuração não é válida. Para obter mais informações, consulte a descrição do evento.

`spotInstanceCountLimitExceeded`

Você atingiu o limite do número de Instâncias spot que você pode executar.

Criar uma regra do Amazon EventBridge

Quando uma notificação de uma alteração de estado é emitida para uma EC2 Fleet ou frota spot, o evento da notificação é enviado para o Amazon EventBridge. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

Você pode escrever uma regra de EventBridge e automatizar quais ações tomar quando o padrão de evento corresponder à regra.

Tópicos

- [Use Amazon EventBridge para monitorar eventos de Frota do EC2 \(p. 808\)](#)
- [Use o Amazon EventBridge para monitorar eventos de frota spot \(p. 811\)](#)

Use Amazon EventBridge para monitorar eventos de Frota do EC2

Quando uma notificação de uma alteração de estado é emitida para uma EC2 Fleet, o evento da notificação é enviado para o Amazon EventBridge na forma de arquivo JSON. Você pode escrever uma regra de EventBridge e automatizar quais ações tomar quando o padrão de evento corresponder à regra. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

Os campos a seguir formam o padrão de evento definido na regra:

`"source": "aws.ec2fleet"`

Identifica que o evento é de Frota do EC2.

`"detail-type": "EC2 Fleet State Change"`

Identifica o tipo de evento.

`"detail": { "sub-type": "submitted" }`

Identifica o subtipo de evento.

Para obter a lista de eventos do EC2 Fleet e dados de eventos de exemplo, consulte [the section called “Tipos de evento de Frota do EC2” \(p. 799\)](#).

Exemplos

- [Criar uma regra de EventBridge para enviar uma notificação \(p. 809\)](#)
- [Criar uma regra de EventBridge para acionar uma função do Lambda \(p. 810\)](#)

Criar uma regra de EventBridge para enviar uma notificação

O exemplo a seguir cria uma regra de EventBridge para enviar um e-mail, mensagem de texto ou notificação por push móvel sempre que o Amazon EC2 emite uma notificação de Frota do EC2. O sinal neste exemplo é emitido como um evento de `EC2 Fleet State Change`, que aciona a ação definida pela regra. Antes de criar a regra EventBridge, você deve criar o tópico do Amazon SNS para e-mail, mensagem de texto ou notificação por push móvel.

Para criar uma regra de EventBridge para enviar uma notificação quando um estado de Frota do EC2 muda

1. Abra o console do Amazon EventBridge em <https://console.aws.amazon.com/events/>.
2. Selecione Criar regra.
3. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.

4. Em Define pattern (Definir padrão), selecione Event pattern (Padrão de evento).
5. Em Event matching pattern (Padrão de correspondência de eventos), você pode escolher Pre-defined pattern by service (Padrão pré-definido por serviço) ou Custom pattern (Padrão personalizado). O Custom pattern (padrão personalizado) permite que você crie uma regra mais detalhada.
 - a. Se você escolher Pre-defined pattern by service (Padrão pré-definido por serviço), faça o seguinte:
 - i. Em Service provider (Provedor de serviços), escolha AWS.
 - ii. Para Service name (Nome do serviço), escolha EC2 Fleet (Frota do EC2).
 - iii. Em Event type (Tipo de evento), selecione o tipo de evento necessário. Para este exemplo, escolha EC2 Fleet Instance Change (Alteração da instância da EC2 Fleet).
 - b. Se você escolher Custom pattern (Padrão personalizado), faça o seguinte:
 - Na caixa Event pattern (Padrão de evento), adicione o seguinte padrão para corresponder ao evento de `EC2 Fleet Instance Change` deste exemplo e escolha Save (Salvar).

```
{  
    "source": ["aws.ec2fleet"],  
    "detail-type": ["EC2 Fleet Instance Change"]  
}
```

6. Em Select event bus (Selecionar barramento de eventos), escolha AWS default event bus (Barramento de eventos padrão da AWS). Quando um serviço da AWS em sua conta emite um evento, ele sempre vai para o barramento de eventos padrão da sua conta.
7. Confirme se Enable the rule on the selected event bus (Habilitar a regra nos barramentos de eventos selecionados) está ativada.
8. Para Target (Destino), escolha SNS topic (tópico SNS) para enviar um e-mail, mensagem de texto ou notificação por push móvel quando o evento ocorrer.
9. Em Topic (Tópico), escolha um tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte [Usar o Amazon SNS para mensagens de aplicação para pessoa \(A2P\)](#) no Guia do desenvolvedor do Amazon Simple Notification Service.

10. Para Configurar entrada, escolha a entrada para e-mail, mensagem de texto ou notificação por push móvel.
11. Escolha Create (Criar).

Para obter mais informações, consulte [Amazon EventBridge rules](#) (Regras do Amazon EventBridge) e [Amazon EventBridge event patterns](#) (Padrões de eventos do Amazon EventBridge) no Amazon EventBridge User Guide (Manual do usuário do Amazon EventBridge).

Criar uma regra de EventBridge para acionar uma função do Lambda

O exemplo a seguir cria uma regra de EventBridge para acionar uma função do Lambda toda vez que Amazon EC2 emite uma notificação de Frota do EC2. O sinal neste exemplo é emitido como um evento de `EC2 Fleet Instance Change`, subtipo `launched`, que aciona a ação definida pela regra. Antes de criar a regra de EventBridge, você deve criar a função do Lambda.

Para criar uma regra de EventBridge para acionar uma função do Lambda quando uma instância em um estado de Frota do EC2 muda

1. Abra o console do AWS Lambda em <https://console.aws.amazon.com/lambda/>.
2. Escolha Create function.
3. Digite um nome para sua função, configure o código e escolha Create function (Criar função).

Para obter mais informações sobre como usar o Lambda, consulte [Create a Lambda function with the console](#) (Criar uma função do Lambda com o console) no AWS Lambda Developer Guide (Guia do desenvolvedor do AWS Lambda).

4. Abra o console do Amazon EventBridge em <https://console.aws.amazon.com/events/>.
5. Selecione Criar regra.
6. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.
7. Em Define pattern (Definir padrão), selecione Event pattern (Padrão de evento).
8. Em Event matching pattern (Padrão de correspondência de eventos), você pode escolher Pre-defined pattern by service (Padrão pré-definido por serviço) ou Custom pattern (Padrão personalizado). O Custom pattern (padrão personalizado) permite que você crie uma regra mais detalhada.
 - a. Se você escolher Pre-defined pattern by service (Padrão pré-definido por serviço), faça o seguinte:
 - i. Em Service provider (Provedor de serviços), escolha AWS.
 - ii. Para Service name (Nome do serviço), escolha EC2 Fleet (Frota do EC2).
 - iii. Em Event type (Tipo de evento), selecione o tipo de evento necessário. Para este exemplo, escolha EC2 Fleet Instance Change (Alteração da instância da EC2 Fleet).
 - b. Se você escolher Custom pattern (Padrão personalizado), faça o seguinte:
 - Na caixa Event pattern (Padrão de evento), adicione o padrão a seguir para corresponder ao `EC2 Fleet Instance Change` evento e `launched` ao subtipo deste exemplo e escolha Save (Salvar).

```
{  
    "source": ["aws.ec2fleet"],  
    "detail-type": ["EC2 Fleet Instance Change"],  
    "detail": {  
        "sub-type": ["launched"]  
    }  
}
```

9. Para Target (Destino), escolha a Lambda function (função Lambda) e, para Function (Função), escolha a função que você criou para responder quando o evento ocorrer.
10. Escolha Create (Criar).

Neste exemplo, a função Lambda será acionada quando o EC2 Fleet Instance Change evento com o subtipo launched ocorrer.

Para obter um tutorial sobre como criar uma função do Lambda e uma EventBridge regra que executa a função do Lambda, consulte [Tutorial: Log the State of an Amazon EC2 Instance Using EventBridge](#) (Tutorial: Registrar o estado de uma instância do Amazon EC2 usando o EventBridge) no AWS Lambda User Guide (Manual do usuário do Amazon EventBridge).

Use o Amazon EventBridge para monitorar eventos de frota spot

Quando uma notificação de alteração de estado é emitida para uma frota spot, o evento da notificação é enviado para o Amazon EventBridge na forma de arquivo JSON. Você pode escrever uma regra de EventBridge e automatizar quais ações tomar quando o padrão de evento corresponder à regra. Se o EventBridge detectar um padrão de evento que corresponda a um padrão definido em uma regra, o EventBridge invocará um destino (ou destinos) especificado(s) na regra.

Os campos a seguir formam o padrão de evento definido na regra:

```
"source": "aws.ec2spotfleet"  
        Identifica que o evento é da frota spot.  
"detail-type": "EC2 Spot Fleet State Change"  
        Identifica o tipo de evento.  
"detail": { "sub-type": "submitted" }  
        Identifica o subtipo de evento.
```

Para obter a lista de eventos Spot Fleet e dados de eventos de exemplo, consulte [the section called “Tipos de evento de frota spot” \(p. 803\)](#).

Exemplos

- [Criar uma regra de EventBridge para enviar uma notificação \(p. 809\)](#)
- [Criar uma regra de EventBridge para acionar uma função do Lambda \(p. 810\)](#)

Criar uma regra de EventBridge para enviar uma notificação

O exemplo a seguir cria uma regra de EventBridge para enviar um e-mail, mensagem de texto ou notificação por push para dispositivos móveis sempre que Amazon EC2 emite uma notificação de frota spot. O sinal neste exemplo é emitido como um evento de EC2 Spot Fleet State Change, que aciona a ação definida pela regra. Antes de criar a regra EventBridge, você deve criar o tópico do Amazon SNS para e-mail, mensagem de texto ou notificação por push móvel.

Para criar uma regra de EventBridge para enviar uma notificação quando o estado de uma Frota spot for alterado

1. Abra o console do Amazon EventBridge em <https://console.aws.amazon.com/events/>.
2. Selecione Criar regra.
3. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.

4. Em Define pattern (Definir padrão), selecione Event pattern (Padrão de evento).
5. Em Event matching pattern (Padrão de correspondência de eventos), você pode escolher Pre-defined pattern by service (Padrão pré-definido por serviço) ou Custom pattern (Padrão personalizado). O Custom pattern (padrão personalizado) permite que você crie uma regra mais detalhada.
 - a. Se você escolher Pre-defined pattern by service (Padrão pré-definido por serviço), faça o seguinte:
 - i. Em Service provider (Provedor de serviços), escolha AWS.
 - ii. Em Service name (Nome do serviço), escolha EC2 Spot Fleet (Frota spot do EC2).
 - iii. Em Event type (Tipo de evento), selecione o tipo de evento necessário. Para este exemplo, escolha EC2 Spot Fleet Instance Change (Alteração da instância da frota spot do EC2).
 - b. Se você escolher Custom pattern (Padrão personalizado), faça o seguinte:
 - Na caixa Event pattern (Padrão de evento), adicione o seguinte padrão para corresponder ao evento de EC2 Spot Fleet Instance Change deste exemplo e escolha Save (Salvar).

```
{  
    "source": ["aws.ec2spotfleet"],  
    "detail-type": ["EC2 Spot Fleet Instance Change"]  
}
```

6. Em Select event bus (Selecionar barramento de eventos), escolha AWS default event bus (Barramento de eventos padrão da AWS). Quando um serviço da AWS em sua conta emite um evento, ele sempre vai para o barramento de eventos padrão da sua conta.
7. Confirme se Enable the rule on the selected event bus (Habilitar a regra nos barramentos de eventos selecionados) está ativada.
8. Para Target (Destino), escolha SNS topic (tópico SNS) para enviar um e-mail, mensagem de texto ou notificação por push móvel quando o evento ocorrer.
9. Em Topic (Tópico), escolha um tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte [Usar o Amazon SNS para mensagens de aplicação para pessoa \(A2P\)](#) no Guia do desenvolvedor do Amazon Simple Notification Service.
10. Para Configurar entrada, escolha a entrada para e-mail, mensagem de texto ou notificação por push móvel.
11. Escolha Create (Criar).

Para obter mais informações, consulte [Amazon EventBridge rules](#) (Regras do Amazon EventBridge) e [Amazon EventBridge event patterns](#) (Padrões de eventos do Amazon EventBridge) no Amazon EventBridge User Guide (Manual do usuário do Amazon EventBridge).

Criar uma regra de EventBridge para acionar uma função do Lambda

O exemplo a seguir cria uma regra de EventBridge para acionar uma função do Lambda sempre que Amazon EC2 emite uma notificação de frota spot. O sinal neste exemplo é emitido como um evento de EC2 Spot Fleet Instance Change, subtipo launched, que aciona a ação definida pela regra. Antes de criar a regra de EventBridge, você deve criar a função do Lambda.

Para criar uma regra de EventBridge para acionar uma função do Lambda quando uma instância de uma Frota spot muda de estado

1. Abra o console do AWS Lambda em <https://console.aws.amazon.com/lambda/>.

2. Escolha Create function.
3. Digite um nome para sua função, configure o código e escolha Create function (Criar função).

Para obter mais informações sobre como usar o Lambda, consulte [Create a Lambda function with the console](#) (Criar uma função do Lambda com o console) no AWS Lambda Developer Guide (Guia do desenvolvedor do AWS Lambda).

4. Abra o console do Amazon EventBridge em <https://console.aws.amazon.com/events/>.
5. Selecione Criar regra.
6. Informe um Name (Nome) para a regra e, opcionalmente, uma descrição.

Uma regra não pode ter o mesmo nome que outra regra na mesma região e no mesmo barramento de eventos.

7. Em Define pattern (Definir padrão), selecione Event pattern (Padrão de evento).
8. Em Event matching pattern (Padrão de correspondência de eventos), você pode escolher Pre-defined pattern by service (Padrão pré-definido por serviço) ou Custom pattern (Padrão personalizado). O Custom pattern (padrão personalizado) permite que você crie uma regra mais detalhada.
 - a. Se você escolher Pre-defined pattern by service (Padrão pré-definido por serviço), faça o seguinte:
 - i. Em Service provider (Provedor de serviços), escolha AWS.
 - ii. Em Service name (Nome do serviço), escolha EC2 Spot Fleet (Frota spot do EC2).
 - iii. Em Event type (Tipo de evento), selecione o tipo de evento necessário. Para este exemplo, escolha EC2 Spot Fleet Instance Change (Alteração da instância da frota spot do EC2).
 - b. Se você escolher Custom pattern (Padrão personalizado), faça o seguinte:
 - Na caixa Event pattern (Padrão de evento), adicione o padrão a seguir para corresponder ao EC2 Spot Fleet Instance Change evento e launchedao subtipo deste exemplo e escolha Save (Salvar).

```
{  
    "source": ["aws.ec2spotfleet"],  
    "detail-type": ["EC2 Spot Fleet Instance Change"],  
    "detail": {  
        "sub-type": ["launched"]  
    }  
}
```

9. Para Target (Destino), escolha a Lambda function (função Lambda) e, para Function (Função), escolha a função que você criou para responder quando o evento ocorrer.
10. Escolha Create (Criar).

Neste exemplo, a função Lambda será acionada quando o EC2 Fleet Instance Change evento com o subtipo launched ocorrer.

Para obter um tutorial sobre como criar uma função do Lambda e uma EventBridge regra que executa a função do Lambda, consulte [Tutorial: Log the State of an Amazon EC2 Instance Using EventBridge](#) (Tutorial: Registrar o estado de uma instância do Amazon EC2 usando o EventBridge) no AWS Lambda User Guide (Manual do usuário do Amazon EventBridge).

Tutoriais para EC2 Fleet e frota spot

Os tutoriais a seguir orientarão você pelos processos comuns de criação de frotas do EC2 e de frotas spot.

Tutoriais

- [Tutorial: Usar a Frota do EC2 com ponderação de instâncias \(p. 814\)](#)
- [Tutorial: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal \(p. 816\)](#)
- [Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas \(p. 817\)](#)
- [Tutorial: Usar frota spot com ponderação de instâncias \(p. 822\)](#)

Tutorial: Usar a Frota do EC2 com ponderação de instâncias

Este tutorial usa uma empresa fictícia chamada Example Corp para ilustrar o processo de solicitação de uma Frota do EC2 usando o peso da instância.

Objective

A Exemplo Corp, uma empresa farmacêutica, quer usar a capacidade computacional do Amazon EC2 para fazer a triagem dos compostos químicos que podem ser usados para combater o câncer.

Planning

Primeiro, a Exemplo Corp analisa as [Melhores práticas de spot](#). Em seguida, a Exemplo Corp determina os requisitos para a Frota do EC2.

Tipos de instância

A Exemplo Corp tem uma aplicação de uso intenso de memória e recursos de computação que funciona melhor com, pelo menos, 60 GB de memória e oito vCPUs virtuais (vCPUs). Eles querem maximizar esses recursos para a aplicação com o menor preço possível. A Exemplo Corp decide que qualquer um dos seguintes tipos de instância do EC2 atenderá às suas necessidades:

Tipo de instância	Memória (GiB)	vCPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacidade de destino em unidades

Com o peso da instância, a capacidade de destino pode igualar um número de instâncias (o padrão) ou uma combinação de fatores, como núcleos (vCPUs), memória (GiB) e armazenamento (GB). Considerando a base para sua aplicação (60 GB de RAM e oito vCPUs) como uma unidade, a Exemplo Corp decide que 20 vezes essa quantidade atenderá às suas necessidades. Então, a empresa define a capacidade de destino da solicitação de Frota do EC2 como 20.

Pesos das instâncias

Depois de determinar a capacidade de destino, a Exemplo Corp calcula os pesos das instâncias. Para calcular o peso para cada tipo de instância, eles determinam as unidades de cada tipo de instância que são necessárias para atingir a capacidade de destino da seguinte forma:

- r3.2xlarge (61,0 GB, 8 vCPUs) = 1 unidade de 20
- r3.4xlarge (122,0 GB, 16 vCPUs) = 2 unidades de 20

- r3.8xlarge (244,0 GB, 32 vCPUs) = 4 unidades de 20

Portanto, a Exemplo Corp atribui os pesos de instância 1, 2 e 4 às respectivas configurações de execução na solicitação de Frota do EC2.

Preço por hora

A Exemplo Corp usa o [Preço sob demanda](#) por hora de instância como o ponto inicial de preço. Eles também podem usar os preços spot recentes ou uma combinação dos dois. Para calcular o preço por hora, eles dividem o preço inicial por hora de instância pelo peso. Por exemplo:

Tipo de instância	Preço sob demanda	Peso da instância	Preço por hora
r3.2xLarge	0,7 USD	1	0,7 USD
r3.4xLarge	1,4 USD	2	0,7 USD
r3.8xLarge	\$2,8	4	0,7 USD

A Exemplo Corp pode usar um preço global por hora de 0,7 USD e ser competitiva para todos os três tipos de instância. Eles também podem usar um preço global por hora de 0,7 USD e um preço específico por hora de 0,9 USD na especificação de execução `r3.8xlarge`.

Verificar permissões

Antes de criar uma Frota do EC2, a Exemplo Corp verifica se ela tem uma função do IAM com as permissões necessárias. Para obter mais informações, consulte [Pré-requisitos da Frota do EC2 \(p. 743\)](#).

Criar um modelo de execução

Em seguida, a Exemplo Corp cria um modelo de execução. O ID do modelo de execução é usado na próxima etapa. Para obter mais informações, consulte [Criar um modelo de execução \(p. 427\)](#).

Criar a Frota do EC2

A Example Corp cria um arquivo, `config.json`, com a seguinte configuração para sua Frota do EC2: No exemplo a seguir, substitua os identificadores de recursos pelos seus identificadores de recursos.

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-07b3bc7625cdab851",  
                "Version": "1"  
            },  
            "Overrides": [  
                {  
                    "InstanceType": "r3.2xlarge",  
                    "SubnetId": "subnet-482e4972",  
                    "WeightedCapacity": 1  
                },  
                {  
                    "InstanceType": "r3.4xlarge",  
                    "SubnetId": "subnet-482e4972",  
                    "WeightedCapacity": 2  
                },  
                {  
                    "InstanceType": "r3.8xlarge",  
                    "SubnetId": "subnet-482e4972",  
                    "WeightedCapacity": 4  
                }  
            ]  
        }  
    ]  
}
```

```
        "MaxPrice": "0.90",
        "SubnetId": "subnet-482e4972",
        "WeightedCapacity": 4
    }
]
},
{
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

A Example Corp cria a Frota do EC2 usando o seguinte comando [create-fleet](#):

```
aws ec2 create-fleet \
--cli-input-json file://config.json
```

Para obter mais informações, consulte [Criar uma Frota do EC2. \(p. 751\)](#).

Fulfillment

A estratégia de alocação determina de quais grupos de capacidade spot os Instâncias spot procedem.

Com a estratégia `lowest-price` (que é uma estratégia padrão), as Instâncias spot vêm do grupo com o menor preço spot por unidade no momento do atendimento. Para fornecer 20 unidades de capacidade, a Frota do EC2 executa 20 instâncias `r3.2xlarge` (20 dividido por 1), 10 instâncias `r3.4xlarge` (20 dividido por 2) ou 5 instâncias `r3.8xlarge` (20 dividido por 4).

Se a Exemplo Corp usasse a estratégia `diversified`, as Instâncias spot viriam dos três grupos. A Frota do EC2 executaria seis instâncias `r3.2xlarge` (que fornecem 6 unidades), três instâncias `r3.4xlarge` (que fornecem 6 unidades), duas instâncias `r3.8xlarge` (que fornecem 8 unidades), totalizando 20 unidades.

Tutorial: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal

Este tutorial usa uma empresa fictícia chamada ABC Online para ilustrar o processo de solicitação de uma Frota do EC2 com opção sob demanda como capacidade principal e capacidade spot (se disponível).

Objective

A ABC Online, uma empresa de entrega para restaurantes, quer provisionar a capacidade do Amazon EC2 em todos os tipos de instâncias do EC2 e opções de compra para atingir a escala, a performance e o custo desejados.

Plan

Ela requer uma capacidade fixa para operar durante períodos de pico, mas gostaria de se beneficiar do aumento da capacidade a um preço menor. A ABC Online determina os seguintes requisitos para suas Frota do EC2:

- Capacidade de instância sob demanda: a ABC Online requer 15 instâncias sob demanda para garantir a acomodação do tráfego em períodos de pico.
- Capacidade de instâncias spot: a ABC Online gostaria de aprimorar a performance, mas com preços mais baixos, com provisionamento de 5 instâncias spot.

Verificar permissões

Antes de criar uma Frota do EC2, a ABC Online verifica se ela tem uma função do IAM com as permissões necessárias. Para obter mais informações, consulte [Pré-requisitos da Frota do EC2 \(p. 743\)](#).

Criar um modelo de execução

O ABC Online cria um modelo de execução. O ID do modelo de execução é usado na próxima etapa. Para obter mais informações, consulte [Criar um modelo de execução \(p. 427\)](#).

Criar a Frota do EC2

A ABC Online cria um arquivo, config.json, com a seguinte configuração para sua Frota do EC2. No exemplo a seguir, substitua os identificadores de recursos pelos seus identificadores de recursos.

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-07b3bc7625cdab851",  
                "Version": "2"  
            }  
        }  
    ],  
    "TargetCapacitySpecification": {  
        "TotalTargetCapacity": 20,  
        "OnDemandTargetCapacity": 15,  
        "DefaultTargetCapacityType": "spot"  
    }  
}
```

A ABC Online cria a Frota do EC2 usando o seguinte comando `create-fleet`:

```
aws ec2 create-fleet \  
  --cli-input-json file://config.json
```

Para obter mais informações, consulte [Criar uma Frota do EC2. \(p. 751\)](#).

Fulfillment

A estratégia de alocação determina que a capacidade sob demanda seja sempre cumprida, enquanto o saldo da capacidade de destino seja atendido como spot se houver capacidade e disponibilidade.

Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas

Este tutorial orienta você por todas as etapas que você deve executar para que sua Frota do EC2 inicie Instâncias sob demanda nas Reservas de Capacidade `targeted`.

Você aprenderá a configurar uma frota para usar as Reservas de Capacidade sob demanda `targeted` primeiro ao iniciar Instâncias sob demanda. Você também aprenderá a configurar a frota para que, quando a capacidade total de destino sob demanda exceder o número de Reservas de Capacidade não utilizadas disponíveis, a frota use a estratégia de alocação especificada para selecionar os grupos de instâncias nos quais iniciar a capacidade de destino restante.

Configuração da Frota do EC2

Nesse tutorial, a configuração da frota é a seguinte:

- Capacidade de destino: 10 Instâncias sob demanda
- Total de Reservas de Capacidade **targeted** não utilizadas: 6 (menor que a capacidade de destino sob demanda da frota de 10 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 2 (**us-east-1a** e **us-east-1b**)
- Número de Reservas de Capacidade por grupo: 3
- Estratégia de alocação sob demanda: **lowest-price** (Quando o número de Reservas de Capacidade não utilizadas for menor que a capacidade de destino sob demanda, a frota determina os grupos nos quais iniciar a capacidade sob demanda restante com base na estratégia de alocação sob demanda.)

Observe que você também pode usar a estratégia de alocação **prioritized** em vez da estratégia de alocação **lowest-price**.

Para iniciar as Instâncias sob demanda em Reservas de Capacidade **targeted**, você deve executar uma série de etapas, da seguinte forma:

- [Etapa 1: Criar Reservas de Capacidade \(p. 818\)](#)
- [Etapa 2: Criar um grupo de recursos de Reservas de capacidade \(p. 819\)](#)
- [Etapa 3: Adicionar as Reservas de Capacidade ao grupo de recursos Reservas de Capacidade \(p. 819\)](#)
- [\(Opcional\) Etapa 4: Exibir Reservas de Capacidade no grupo de recursos \(p. 819\)](#)
- [Etapa 5: Criar um modelo de inicialização que especifique que a Reserva de Capacidade se destina a um grupo de recursos específico \(p. 820\)](#)
- [\(Opcional\) Etapa 6: Descrever o modelo de inicialização \(p. 820\)](#)
- [Etapa 7: Criar uma Frota EC2 \(p. 821\)](#)
- [\(Opcional\) Etapa 8: Exibir o número de Reservas de Capacidade não utilizadas restantes \(p. 822\)](#)

Etapa 1: Criar Reservas de Capacidade

Use o comando [Create-capacity-reservation](#) para criar as Reservas de Capacidade, três para **us-east-1a** e outras três para **us-east-1b**. Exceto para a Zona de disponibilidade, os outros atributos das Reservas de Capacidade são idênticos.

3 Reservas de Capacidade no **us-east-1a**

```
aws ec2 create-capacity-reservation \
--availability-zone us-east-1a \
--instance-type c5.xlarge \
--instance-platform Linux/UNIX \
--instance-count 3 \
--instance-match-criteria targeted
```

Exemplo de ID de reserva de capacidade resultante

```
cr-1234567890abcdef1
```

3 Reservas de Capacidade no **us-east-1b**

```
aws ec2 create-capacity-reservation \
--availability-zone us-east-1b \
--instance-type c5.xlarge \
--instance-platform Linux/UNIX \
--instance-count 3 \
```

```
--instance-match-criteria targeted
```

Exemplo de ID de reserva de capacidade resultante

```
cr-54321abcdef567890
```

Etapa 2: Criar um grupo de recursos de Reservas de capacidade

Use o serviço `resource-groups` e o comando `create-group` para criar um grupo de recursos de Reservas de capacidade. Neste exemplo, o grupo de recursos é chamado de `my-cr-group`. Para obter informações sobre por que você deve criar um grupo de recursos, consulte [Use Reservas de Capacidade para Instâncias on-demand \(p. 736\)](#).

```
aws resource-groups create-group \  
  --name my-cr-group \  
  --configuration '{ "Type": "AWS::EC2::CapacityReservationPool" }' \  
  '{ "Type": "AWS::ResourceGroups::Generic", "Parameters": [ { "Name": "allowed-resource-types", "Values": [ "AWS::EC2::CapacityReservation" ] } ] }'
```

Etapa 3: Adicionar as Reservas de Capacidade ao grupo de recursos Reservas de Capacidade

Use o serviço `resource-groups` e o comando `group-resources` para adicionar as Reservas de Capacidade que você criou na Etapa 1 para o grupo de recursos Reservas de Capacidade. Observe que você deve fazer referência às Reservas de Capacidade sob demanda por seus ARNs.

```
aws resource-groups group-resources \  
  --group my-cr-group \  
  --resource-arns \  
    arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \  
    arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Exemplo de saída

```
{  
  "Failed": [],  
  "Succeeded": [  
    "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",  
    "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"  
  ]  
}
```

(Opcional) Etapa 4: Exibir Reservas de Capacidade no grupo de recursos

Use o serviço `resource-groups` e o comando `list-group-resources` para descrever opcionalmente o grupo de recursos para exibir suas Reservas de Capacidade.

```
aws resource-groups list-group-resources --group my-cr-group
```

Exemplo de saída

```
{  
  "ResourceIdentifiers": [  
    {
```

```
"ResourceType": "AWS::EC2::CapacityReservation",
"ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
},
{
    "ResourceType": "AWS::EC2::CapacityReservation",
    "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
}
]
```

Etapa 5: Criar um modelo de inicialização que especifique que a Reserva de Capacidade se destina a um grupo de recursos específico

Use o comando [create-launch-template](#) para criar um modelo de execução no qual especifique as Reservas de Capacidade a serem usadas. Neste exemplo, a frota usará Reservas de Capacidade `targeted`, que foram adicionadas a um grupo de recursos. Portanto, os dados do modelo de inicialização especificam que a Reserva de Capacidade se destina a um grupo de recursos específico. Neste exemplo, o modelo de inicialização é chamado de `my-launch-template`.

```
aws ec2 create-launch-template \
--launch-template-name my-launch-template \
--launch-template-data \
'{ "ImageId": "ami-0123456789example",  
  "CapacityReservationSpecification":  
    { "CapacityReservationTarget":  
      { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-cr-group" }  
    }  
'
```

(Opcional) Etapa 6: Descrever o modelo de inicialização

Use o comando [template describe-launch-template](#) para descrever opcionalmente o modelo de lançamento para exibir sua configuração.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Exemplo de saída

```
{  
    "LaunchTemplateVersions": [  
        {  
            "LaunchTemplateId": "lt-01234567890example",  
            "LaunchTemplateName": "my-launch-template",  
            "VersionNumber": 1,  
            "CreateTime": "2021-01-19T20:50:19.000Z",  
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",  
            "DefaultVersion": true,  
            "LaunchTemplateData": {  
                "ImageId": "ami-0947d2ba12ee1ff75",  
                "CapacityReservationSpecification": {  
                    "CapacityReservationTarget": {  
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-cr-group"  
                    }  
                }  
            }  
        }  
    ]  
}
```

```
        }
    ]
}
```

Etapa 7: Criar uma Frota EC2

Crie uma EC2 Fleet que especifique as informações de configuração para as instâncias que serão iniciadas. A configuração de frota EC2 a seguir mostra somente as configurações pertinentes a esse exemplo. O modelo de inicialização `my-launch-template` é o modelo de inicialização criado na Etapa 5. Há dois grupos de instâncias, cada um com o mesmo tipo de instância (`c5.xlarge`), mas com diferentes zonas de disponibilidade (`us-east-1a` e `us-east-1b`). O preço dos grupos de instâncias é o mesmo porque o preço é definido para a Região, não para a Zona de Disponibilidade. A capacidade de destino total é de 10 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

Note

O tipo da frota deve ser `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
                {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
                }
            ]
        },
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 10,
            "DefaultTargetCapacityType": "on-demand"
        },
        "OnDemandOptions": {
            "AllocationStrategy": "lowest-price",
            "CapacityReservationOptions": {
                "UsageStrategy": "use-capacity-reservations-first"
            }
        },
        "Type": "instant"
    }
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 10 instâncias a seguir serão iniciadas para atender à capacidade de destino:

- As Reservas de Capacidade são usadas primeiro para iniciar 6 Instâncias sob demanda da seguinte maneira:
 - 3 Instâncias sob demanda são iniciadas nas 3 `c5.xlarge` Reservas de Capacidade `targeted` no `us-east-1a`

- 3 Instâncias sob demanda são iniciadas nas 3 c5.xlarge Reservas de Capacidade `targeted` no `us-east-1b`
- Para atender à capacidade de destino, 4 Instâncias sob demanda adicionais são iniciadas na capacidade sob demanda regular de acordo com a estratégia de alocação sob demanda, que é `lowest-price` neste exemplo. No entanto, como os grupos têm o mesmo preço (porque o preço é por Região e não por zona de disponibilidade), a frota inicia as 4 Instâncias sob demanda restantes em qualquer um dos grupos.

(Opcional) Etapa 8: Exibir o número de Reservas de Capacidade não utilizadas restantes

Depois que a frota for lançada, você poderá, opcionalmente, executar `describe-capacity-reservations` para ver quantas Reservas de Capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade foram usadas em todos os grupos.

```
{ "CapacityReservationId": "cr-111",
  "InstanceType": "c5.xlarge",
  "AvailableInstanceCount": 0
}

{ "CapacityReservationId": "cr-222",
  "InstanceType": "c5.xlarge",
  "AvailableInstanceCount": 0
}
```

Tutorial: Usar frota spot com ponderação de instâncias

Este tutorial usa uma empresa fictícia chamada Example Corp para ilustrar o processo de solicitação de uma frota spot usando o peso da instância.

Objective

A Exemplo Corp, uma empresa farmacêutica, quer impulsionar a capacidade computacional do Amazon EC2 para fazer a triagem dos compostos químicos que podem ser usados para combater o câncer.

Planning

Primeiro, a Exemplo Corp analisa as [Melhores práticas de spot](#). Em seguida, a Exemplo Corp determina os seguintes requisitos para a frota spot.

Tipos de instância

A Exemplo Corp tem uma aplicação de uso intenso de memória e recursos de computação que funciona melhor com, pelo menos, 60 GB de memória e oito CPUs virtuais (vCPUs). Eles querem maximizar esses recursos para a aplicação com o menor preço possível. A Exemplo Corp decide que qualquer um dos seguintes tipos de instância do EC2 atenderá às suas necessidades:

Tipo de instância	Memória (GiB)	vCPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Capacidade de destino em unidades

Com o peso da instância, a capacidade de destino pode igualar um número de instâncias (o padrão) ou uma combinação de fatores, como núcleos (vCPUs), memória (GiB) e armazenamento (GB). Considerando a base para sua aplicação (60 GB de RAM e oito vCPUs) como 1 unidade, a Exemplo Corp decide que 20 vezes essa quantidade atenderá às suas necessidades. Então, a empresa define a capacidade de destino da solicitação de frota spot como 20.

Pesos das instâncias

Depois de determinar a capacidade de destino, a Exemplo Corp calcula os pesos das instâncias. Para calcular o peso para cada tipo de instância, eles determinam as unidades de cada tipo de instância que são necessárias para atingir a capacidade de destino da seguinte forma:

- r3.2xlarge (61,0 GB, 8 vCPUs) = 1 unidade de 20
- r3.4xlarge (122,0 GB, 16 vCPUs) = 2 unidades de 20
- r3.8xlarge (244,0 GB, 32 vCPUs) = 4 unidades de 20

Portanto, a Exemplo Corp atribui os pesos de instância 1, 2 e 4 às respectivas configurações de execução na solicitação de frota spot.

Preço por hora

A Exemplo Corp usa o [Preço sob demanda](#) por hora de instância como o ponto inicial de preço. Eles também podem usar os preços spot recentes ou uma combinação dos dois. Para calcular o preço por hora, eles dividem o preço inicial por hora de instância pelo peso. Por exemplo:

Tipo de instância	Preço sob demanda	Peso da instância	Preço por hora
r3.2xLarge	0,7 USD	1	0,7 USD
r3.4xLarge	1,4 USD	2	0,7 USD
r3.8xLarge	\$2,8	4	0,7 USD

A Exemplo Corp pode usar um preço global por hora de 0,7 USD e ser competitiva para todos os três tipos de instância. Eles também podem usar um preço global por hora de 0,7 USD e um preço específico por hora de 0,9 USD na especificação de execução `r3.8xlarge`.

Verificar permissões

Antes de criar uma solicitação de frota spot, a Exemplo Corp verifica se ela tem uma função do IAM com as permissões necessárias. Para obter mais informações, consulte [Permissões de frota spot \(p. 771\)](#).

Criar a solicitação

A Exemplo Corp cria um arquivo, `config.json`, com a seguinte configuração para sua solicitação de frota spot:

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.8xlarge",  
            "MinCount": 1,  
            "MaxCount": 20,  
            "WeightedCapacity": 4  
        }  
    ]  
}
```

```
"InstanceType": "r3.2xlarge",
"SubnetId": "subnet-482e4972",
"WeightedCapacity": 1
},
{
  "ImageId": "ami-1a2b3c4d",
  "InstanceType": "r3.4xlarge",
  "SubnetId": "subnet-482e4972",
  "WeightedCapacity": 2
},
{
  "ImageId": "ami-1a2b3c4d",
  "InstanceType": "r3.8xlarge",
  "SubnetId": "subnet-482e4972",
  "SpotPrice": "0.90",
  "WeightedCapacity": 4
}
]
```

A Exemplo Corp cria a solicitação de frota spot usando o comando [request-spot-fleet](#).

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Para obter mais informações, consulte [Tipos de solicitação da frota spot \(p. 761\)](#).

Fulfillment

A estratégia de alocação determina de quais grupos de capacidade spot os Instâncias spot procedem.

Com a estratégia `lowestPrice` (que é uma estratégia padrão), as Instâncias spot vêm do grupo com o menor preço spot por unidade no momento do atendimento. Para fornecer 20 unidades de capacidade, a frota spot executa 20 instâncias `r3.2xlarge` (20 dividido por 1), 10 instâncias `r3.4xlarge` (20 dividido por 2) ou 5 instâncias `r3.8xlarge` (20 dividido por 4).

Se a Exemplo Corp usasse a estratégia `diversified`, as Instâncias spot viriam dos três grupos. A frota spot executaria seis instâncias `r3.2xlarge` (que fornecem 6 unidades), três instâncias `r3.4xlarge` (que fornecem 6 unidades), duas instâncias `r3.8xlarge` (que fornecem 8 unidades), totalizando 20 unidades.

Exemplo de configurações para EC2 Fleet e frota spot

Os exemplos a seguir mostram configurações de execução que você pode usar para criar frotas do EC2 e frotas spot.

Tópicos

- [Exemplos de configuração de Frota do EC2 \(p. 824\)](#)
- [Exemplos de configuração de frota spot \(p. 837\)](#)

Exemplos de configuração de Frota do EC2

Os exemplos a seguir mostram configurações de execução que você pode usar com o comando `create-fleet` para criar uma Frota do EC2. Para obter mais informações sobre os parâmetros `criar-fleet`, consulte a [Referência do arquivo de configuração JSON da Frota do EC2 \(p. 747\)](#).

Exemplos

- [Exemplo 1: Executar Instâncias spot como a opção de compra padrão \(p. 825\)](#)
- [Exemplo 2: Executar Instâncias on-demand como a opção de compra padrão \(p. 825\)](#)
- [Exemplo 3: Executar Instâncias on-demand como a capacidade principal \(p. 826\)](#)
- [Exemplo 4: Iniciar Instâncias spot usando a estratégia de alocação lowest-price \(p. 826\)](#)
- [Exemplo 5: Iniciar Instâncias sob demanda usando várias Reservas de Capacidade \(p. 827\)](#)
- [Exemplo 6: Iniciar Instâncias sob demanda usando Reservas de Capacidade quando a capacidade total de destino for maior que o número de Reservas de Capacidade não utilizadas \(p. 829\)](#)
- [Exemplo 7: Iniciar Instâncias sob demanda usando Reservas de Capacidade direcionadas \(p. 832\)](#)
- [Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição \(p. 834\)](#)
- [Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade \(p. 835\)](#)
- [Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades \(p. 836\)](#)

Exemplo 1: Executar Instâncias spot como a opção de compra padrão

O exemplo a seguir especifica os parâmetros mínimos necessários em uma Frota do EC2: um modelo de execução, a capacidade de destino e a opção de compra padrão. O modelo de execução é identificado pelo ID do seu modelo de execução e o número da versão. A capacidade de destino da frota é de 2 instâncias, e a opção de compra padrão é spot. Isso faz com que a frota execute duas Instâncias spot.

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-0e8c754449b27161c",  
                "Version": "1"  
            }  
        },  
        {  
            "TargetCapacitySpecification": {  
                "TotalTargetCapacity": 2,  
                "DefaultTargetCapacityType": "spot"  
            }  
        }  
    ]  
}
```

Exemplo 2: Executar Instâncias on-demand como a opção de compra padrão

O exemplo a seguir especifica os parâmetros mínimos necessários em uma Frota do EC2: um modelo de execução, a capacidade de destino e a opção de compra padrão. O modelo de execução é identificado pelo ID do seu modelo de execução e o número da versão. A capacidade de destino da frota é de 2 instâncias, e a opção de compra padrão é on-demand. Isso faz com que a frota execute duas Instâncias on-demand.

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-0e8c754449b27161c",  
                "Version": "1"  
            }  
        }  
    ]  
}
```

```
        },
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

Exemplo 3: Executar Instâncias on-demand como a capacidade principal

O exemplo a seguir especifica a capacidade total de destino de duas instâncias para a frota e uma capacidade de destino de uma instância sob demanda. A opção de compra padrão é spot. A frota executa uma instância sob demanda, conforme especificado, mas precisa executar mais uma instância para atender à capacidade total desejada. A opção de compra para a diferença é calculada como $\text{TotalTargetCapacity} - \text{OnDemandTargetCapacity} = \text{DefaultTargetCapacityType}$. Isso faz com que a frota execute uma instância spot.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Exemplo 4: Iniciar Instâncias spot usando a estratégia de alocação lowest-price

Se a estratégia de alocação para Instâncias spot não for especificada, a estratégia de alocação padrão, `lowest-price`, será usada. O exemplo a seguir usa a estratégia de alocação `lowest-price`. As três especificações de execução, que substituem o modelo de execução, têm tipos de instância diferentes, mas a mesma capacidade ponderada e sub-rede. A capacidade de destino total é de duas instâncias, e a opção de compra padrão é spot. A Frota do EC2 executa duas Instâncias spot usando o tipo de instância da especificação de execução com o menor preço.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
        }
    ],
    "Overrides": [
        {
            "InstanceType": "c4.large",
            "WeightedCapacity": 1,
            "SubnetId": "subnet-a4f6c5d3"
        }
    ]
}
```

```
        },
        {
            "InstanceType": "c3.large",
            "WeightedCapacity": 1,
            "SubnetId": "subnet-a4f6c5d3"
        },
        {
            "InstanceType": "c5.large",
            "WeightedCapacity": 1,
            "SubnetId": "subnet-a4f6c5d3"
        }
    ]
}

],
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 2,
    "DefaultTargetCapacityType": "spot"
}
}
```

Exemplo 5: Iniciar Instâncias sob demanda usando várias Reservas de Capacidade

É possível configurar uma frota para usar Reservas de Capacidade sob demanda primeiro ao iniciar Instâncias on-demand definindo a estratégia de uso para Reservas de Capacidade como `use-capacity-reservations-first`. Este exemplo demonstra como a frota seleciona as Reservas de Capacidade a serem usadas quando há mais Reservas de Capacidade do que o necessário para atender à capacidade de destino.

Neste exemplo, a configuração da frota é a seguinte:

- Capacidade de destino: 12 Instâncias sob demanda
- Total de Reservas de Capacidade não utilizadas: 15 (mais do que a capacidade de destino da frota de 12 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)
- Número de Reservas de Capacidade por grupo: 5
- Estratégia de alocação sob demanda: `lowest-price` (Quando há várias Reservas de Capacidade não utilizadas em vários grupos de instâncias, a frota determina os grupos nos quais as Instâncias sob demanda serão iniciadas com base na estratégia de alocação sob demanda.)

Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Capacity Reservations

A conta tem as 15 Reservas de Capacidade não utilizadas a seguir em 3 grupos diferentes. O número de Reservas de Capacidade em cada grupo é indicado por `AvailableInstanceCount`.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

```
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "m4.xlarge",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 5,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}  
  
{  
    "CapacityReservationId": "cr-333",  
    "InstanceType": "m4.2xlarge",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 5,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}
```

Configuração da frota

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A capacidade de destino total é de 12 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-capacity-reservations-first`.

Neste exemplo, o preço da instância sob demanda é:

- `m5.large` – 0,096 USD por hora
- `m4.xlarge` – 0,20 USD por hora
- `m4.2xlarge` – 0,40 USD por hora

Note

O tipo da frota deve ser do tipo `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-abc1234567example",  
                "Version": "1"  
            }  
            "Overrides": [  
                {  
                    "InstanceType": "m5.large",  
                    "AvailabilityZone": "us-east-1a",  
                    "WeightedCapacity": 1  
                },  
                {  
                    "InstanceType": "m4.xlarge",  
                    "AvailabilityZone": "us-east-1a",  
                    "WeightedCapacity": 1  
                },  
                {  
                    "InstanceType": "m4.2xlarge",  
                    "AvailabilityZone": "us-east-1a",  
                    "WeightedCapacity": 1  
                }  
            ]  
        }  
    ]  
}
```

```
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Depois de criar a frota instant usando a configuração anterior, as 12 instâncias a seguir serão executadas para atender à capacidade de destino:

- 5 m5.large Instâncias sob demanda em us-east-1a – m5.large em us-east-1a é o preço mais baixo, e há 5 Reservas de Capacidade m5.large disponíveis não utilizadas
- 5 m4.xlarge Instâncias sob demanda em m4.xlarge – us-east-1a em us-east-1a é o próximo preço mais baixo, e há 5 Reservas de Capacidade m4.xlarge não utilizadas disponíveis
- 2 Instâncias sob demanda m4.2xlarge em us-east-1a – m4.2xlarge em us-east-1a é o terceiro preço mais baixo, e existem 5 Reservas de Capacidade m4.2xlarge não utilizadas disponíveis, das quais somente 2 são necessárias para atender à capacidade de destino

Depois que a frota for lançada, você poderá executar [describe-capacity-reservations](#) para ver quantas Reservas de Capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade m5.large e m4.xlarge foram usadas, com 3 Reservas de Capacidade m4.2xlarge restantes não utilizadas.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

Exemplo 6: Iniciar Instâncias sob demanda usando Reservas de Capacidade quando a capacidade total de destino for maior que o número de Reservas de Capacidade não utilizadas

É possível configurar uma frota para usar Reservas de Capacidade sob demanda primeiro ao iniciar Instâncias on-demand definindo a estratégia de uso para Reservas de Capacidade como `use-capacity-`

`reservations-first`. Este exemplo demonstra como a frota seleciona os grupos de instâncias nos quais iniciar Instâncias sob demanda quando a capacidade total de destino excede o número de Reservas de Capacidade não utilizadas disponíveis.

Neste exemplo, a configuração da frota é a seguinte:

- Capacidade de destino: 16 Instâncias sob demanda
- Total de Reservas de Capacidade não utilizadas: 15 (menor que a capacidade de destino da frota de 16 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 3 (`m5.large`, `m4.xlarge` e `m4.2xlarge`)
- Número de Reservas de Capacidade por grupo: 5
- Estratégia de alocação sob demanda: `lowest-price` (Quando o número de Reservas de Capacidade não utilizadas for menor que a capacidade de destino sob demanda, a frota determina os grupos nos quais iniciar a capacidade sob demanda restante com base na estratégia de alocação sob demanda.)

Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Capacity Reservations

A conta tem as 15 Reservas de Capacidade não utilizadas a seguir em 3 grupos diferentes. O número de Reservas de Capacidade em cada grupo é indicado por `AvailableInstanceCount`.

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "m5.large",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 5,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}  
  
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "m4.xlarge",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 5,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}  
  
{  
    "CapacityReservationId": "cr-333",  
    "InstanceType": "m4.2xlarge",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 5,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}
```

Configuração da frota

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A capacidade de destino total é de 16 e o tipo de capacidade de destino padrão é `on-demand`. A estratégia de alocação sob demanda é `lowest-price`. A estratégia de uso para Reservas de Capacidade é `use-reservations-first`.

Neste exemplo, o preço da instância sob demanda é:

- m5.large – 0,096 USD por hora
- m4.xlarge – 0,20 USD por hora
- m4.2xlarge – 0,40 USD por hora

Note

O tipo da frota deve ser `instant`. Outros tipos de frota não são compatíveis com `use-capacity-reservations-first`.

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateId": "lt-0e8c754449b27161c",  
                "Version": "1"  
            }  
            "Overrides": [  
                {  
                    "InstanceType": "m5.large",  
                    "AvailabilityZone": "us-east-1a",  
                    "WeightedCapacity": 1  
                },  
                {  
                    "InstanceType": "m4.xlarge",  
                    "AvailabilityZone": "us-east-1a",  
                    "WeightedCapacity": 1  
                },  
                {  
                    "InstanceType": "m4.2xlarge",  
                    "AvailabilityZone": "us-east-1a",  
                    "WeightedCapacity": 1  
                }  
            ]  
        }  
    ],  
    "TargetCapacitySpecification": {  
        "TotalTargetCapacity": 16,  
        "DefaultTargetCapacityType": "on-demand"  
    },  
    "OnDemandOptions": {  
        "AllocationStrategy": "lowest-price"  
        "CapacityReservationOptions": {  
            "UsageStrategy": "use-capacity-reservations-first"  
        }  
    },  
    "Type": "instant",  
}
```

Depois de criar a frota `instant` usando a configuração anterior, as 16 instâncias a seguir serão executadas para atender à capacidade de destino:

- 6 Instâncias sob demanda `m5.large` em `us-east-1a` – `m5.large` em `us-east-1a` é o preço mais baixo, e há 5 Reservas de Capacidade `m5.large` disponíveis não utilizadas As Reservas de Capacidade são usadas primeiro para iniciar 5 Instâncias sob demanda. Depois das Reservas de Capacidade `m4.xlarge` e `m4.2xlarge` restantes serem usadas, para atender à capacidade de destino, uma instância sob demanda adicional é iniciada, de acordo com a estratégia de alocação sob demanda, que é `lowest-price` neste exemplo.

- 5 m4.xlarge Instâncias sob demanda em us-east-1a – m4.xlarge em us-east-1a é o próximo preço mais baixo, e há 5 Reservas de Capacidade m4.xlarge disponíveis não utilizadas
- 5 m4.2xlarge Instâncias sob demanda em us-east-1a – m4.2xlarge em us-east-1a é o terceiro preço mais baixo, e há 5 Reservas de Capacidade m4.2xlarge disponíveis não utilizadas

Depois que a frota for lançada, você poderá executar [describe-capacity-reservations](#) para ver quantas Reservas de Capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade foram usadas em todos os grupos.

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "m5.large",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "m4.xlarge",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-333",  
    "InstanceType": "m4.2xlarge",  
    "AvailableInstanceCount": 0  
}
```

Exemplo 7: Iniciar Instâncias sob demanda usando Reservas de Capacidade direcionadas

É possível configurar uma frota para usar Reservas de Capacidade `targeted` sob demanda primeiro ao iniciar Instâncias sob demanda definindo a estratégia de uso para Reservas de Capacidade como `use-capacity-reservations-first`. Este exemplo demonstra como iniciar Instâncias sob demanda nas Reservas de Capacidade `targeted`, com os atributos das Reservas de Capacidade sendo os mesmos, exceto para suas Zonas de Disponibilidade (us-east-1a e us-east-1b). Ele também demonstra como a frota seleciona os grupos de instâncias nos quais iniciar Instâncias sob demanda quando a capacidade total de destino excede o número de Reservas de Capacidade não utilizadas disponíveis.

Neste exemplo, a configuração da frota é a seguinte:

- Capacidade de destino: 10 Instâncias sob demanda
- Total de Reservas de Capacidade `targeted` não utilizadas: 6 (menor que a capacidade de destino sob demanda da frota de 10 Instâncias sob demanda)
- Número de grupos de Reservas de capacidade: 2 (us-east-1a e us-east-1b)
- Número de Reservas de Capacidade por grupo: 3
- Estratégia de alocação sob demanda: `lowest-price` (Quando o número de Reservas de Capacidade não utilizadas for menor que a capacidade de destino sob demanda, a frota determina os grupos nos quais iniciar a capacidade sob demanda restante com base na estratégia de alocação sob demanda.)

Observe que você também pode usar a estratégia de alocação `prioritized` em vez da estratégia de alocação `lowest-price`.

Para obter uma demonstração dos procedimentos que você deve executar para realizar este exemplo, consulte [Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas \(p. 817\)](#).

Capacity Reservations

A conta tem as 6 Reservas de Capacidade não utilizadas a seguir em 2 grupos diferentes. Neste exemplo, os grupos diferem de acordo com suas Zonas de disponibilidade. O número de Reservas de Capacidade em cada grupo é indicado por AvailableInstanceCount.

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "c5.xlarge",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1a",  
    "AvailableInstanceCount": 3,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}  
  
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "c5.xlarge",  
    "InstancePlatform": "Linux/UNIX",  
    "AvailabilityZone": "us-east-1b",  
    "AvailableInstanceCount": 3,  
    "InstanceMatchCriteria": "open",  
    "State": "active"  
}
```

Configuração da frota

A configuração de frota a seguir mostra somente as configurações pertinentes a este exemplo. A capacidade de destino total é de 10 e o tipo de capacidade de destino padrão é on-demand. A estratégia de alocação sob demanda é lowest-price. A estratégia de uso para Reservas de Capacidade é use-capacity-reservations-first.

Neste exemplo, o preço da instância sob demanda para c5.xlarge em us-east-1 é 0,17 USD por hora.

Note

O tipo da frota deve ser instant. Outros tipos de frota não são compatíveis com use-capacity-reservations-first.

```
{  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateName": "my-launch-template",  
                "Version": "1"  
            },  
            "Overrides": [  
                {  
                    "InstanceType": "c5.xlarge",  
                    "AvailabilityZone": "us-east-1a"  
                },  
                {  
                    "InstanceType": "c5.xlarge",  
                    "AvailabilityZone": "us-east-1b"  
                }  
            ]  
        }  
    ],  
    "TargetCapacitySpecification": {  
        "TotalTargetCapacity": 10,  
        "DefaultTargetCapacityType": "on-demand"  
    },  
    "OnDemandOptions": {  
        "AllocationStrategy": "lowest-price",  
        "AllocationCount": 10  
    }  
}
```

```
    "CapacityReservationOptions": {  
        "UsageStrategy": "use-capacity-reservations-first"  
    }  
},  
"Type": "instant"  
}
```

Depois de criar a frota instant usando a configuração anterior, as 10 instâncias a seguir serão iniciadas para atender à capacidade de destino:

- As Reservas de Capacidade são usadas primeiro para iniciar 6 Instâncias sob demanda da seguinte maneira:
 - 3 Instâncias sob demanda são iniciadas nas 3 c5.xlarge Reservas de Capacidade targeted no us-east-1a
 - 3 Instâncias sob demanda são iniciadas nas 3 c5.xlarge Reservas de Capacidade targeted no us-east-1b
- Para atender à capacidade de destino, 4 Instâncias sob demanda adicionais são iniciadas na capacidade sob demanda regular de acordo com a estratégia de alocação sob demanda, que é lowest-price neste exemplo. No entanto, como os grupos têm o mesmo preço (porque o preço é por Região e não por zona de disponibilidade), a frota inicia as 4 Instâncias sob demanda restantes em qualquer um dos grupos.

Depois que a frota for lançada, você poderá executar [describe-capacity-reservations](#) para ver quantas Reservas de Capacidade não utilizadas restam. Neste exemplo, você deve ver a resposta a seguir, que mostra que todas as Reservas de Capacidade foram usadas em todos os grupos.

```
{  
    "CapacityReservationId": "cr-111",  
    "InstanceType": "c5.xlarge",  
    "AvailableInstanceCount": 0  
}  
  
{  
    "CapacityReservationId": "cr-222",  
    "InstanceType": "c5.xlarge",  
    "AvailableInstanceCount": 0  
}
```

Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição

O exemplo a seguir configura a EC2 Fleet para executar uma Instância spot de substituição quando o Amazon EC2 emite uma recomendação de rebalanceamento para uma Instância spot na frota. Para configurar a substituição automática da Instâncias spot, para `ReplacementStrategy`, especifique `launch`.

Note

Quando uma instância de substituição é executada, a instância marcada para rebalanceamento não é automaticamente encerrada. Você pode encerrá-la, ou você pode deixá-la em funcionamento. Você é cobrado por ambas as instâncias enquanto elas estão sendo executadas.

A eficácia da estratégia de rebalanceamento de capacidade depende do número de grupos de capacidade spot especificados na solicitação de Frota do EC2. Recomendamos que você configure a frota com um conjunto diversificado de tipos de instância e zonas de disponibilidade e para `AllocationStrategy` especifique `capacity-optimized`. Para obter mais informações sobre o que

você deve considerar ao configurar uma Frota do EC2 para rebalanceamento de capacidade, consulte [Rebalanceamento de capacidade \(p. 737\)](#).

```
{  
    "ExcessCapacityTerminationPolicy": "termination",  
    "LaunchTemplateConfigs": [  
        {  
            "LaunchTemplateSpecification": {  
                "LaunchTemplateName": "LaunchTemplate",  
                "Version": "1"  
            },  
            "Overrides": [  
                {  
                    "InstanceType": "c3.large",  
                    "WeightedCapacity": 1,  
                    "Placement": {  
                        "AvailabilityZone": "us-east-1a"  
                    }  
                },  
                {  
                    "InstanceType": "c4.large",  
                    "WeightedCapacity": 1,  
                    "Placement": {  
                        "AvailabilityZone": "us-east-1a"  
                    }  
                },  
                {  
                    "InstanceType": "c5.large",  
                    "WeightedCapacity": 1,  
                    "Placement": {  
                        "AvailabilityZone": "us-east-1a"  
                    }  
                }  
            ]  
        },  
        {  
            "TargetCapacitySpecification": {  
                "TotalTargetCapacity": 5,  
                "DefaultTargetCapacityType": "spot"  
            },  
            "SpotOptions": {  
                "AllocationStrategy": "capacity-optimized",  
                "MaintenanceStrategies": {  
                    "CapacityRebalance": {  
                        "ReplacementStrategy": "launch"  
                    }  
                }  
            }  
        }  
    ]  
},  
"SpotOptions": {  
    "AllocationStrategy": "capacity-optimized",  
    "MaintenanceStrategies": {  
        "CapacityRebalance": {  
            "ReplacementStrategy": "launch"  
        }  
    }  
}
```

Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade

O exemplo a seguir demonstra como configurar uma EC2 Fleet com uma estratégia de alocação spot que optimiza a capacidade. Para optimizar a capacidade, você deve definir AllocationStrategy como capacity-optimized.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A EC2 Fleet tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias em execução.

```
{
```

```
"SpotOptions": {  
    "AllocationStrategy": "capacity-optimized",  
},  
"LaunchTemplateConfigs": [  
    {  
        "LaunchTemplateSpecification": {  
            "LaunchTemplateName": "my-launch-template",  
            "Version": "1"  
        },  
        "Overrides": [  
            {  
                "InstanceType": "r4.2xlarge",  
                "Placement": {  
                    "AvailabilityZone": "us-west-2a"  
                },  
            },  
            {  
                "InstanceType": "m4.2xlarge",  
                "Placement": {  
                    "AvailabilityZone": "us-west-2b"  
                },  
            },  
            {  
                "InstanceType": "c5.2xlarge",  
                "Placement": {  
                    "AvailabilityZone": "us-west-2b"  
                }  
            }  
        ]  
    },  
],  
"TargetCapacitySpecification": {  
    "TotalTargetCapacity": 50,  
    "DefaultTargetCapacityType": "spot"  
}
```

Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades

O exemplo a seguir demonstra como configurar uma EC2 Fleet com uma estratégia de alocação spot que optimiza a capacidade enquanto usa a prioridade com base no melhor esforço.

Ao usar a estratégia de alocação `capacity-optimized-prioritized`, você pode usar o parâmetro `Priority` para especificar as prioridades dos grupos de capacidade spot, em que quanto menor o número, maior a prioridade. Você também pode definir a mesma prioridade para vários grupos de capacidade spot se você favorecer os igualmente. Se você não definir uma prioridade para um grupo, ele será considerado o último em termos de prioridade.

Para priorizar grupos de capacidade spot, você deve definir `AllocationStrategy` como `capacity-optimized-prioritized`. A EC2 Fleet otimizará a capacidade primeiro, mas se empenhará em honrar as prioridades (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da EC2 Fleet de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. Cada grupo é priorizado, onde quanto menor o número, maior a prioridade. A capacidade pretendida é de 50 Instâncias spot. A EC2 Fleet tenta executar 50 instâncias Spot no grupo de capacidade spot com a maior prioridade com base no melhor esforço, mas optimiza a capacidade em primeiro lugar.

```
{  
    "SpotOptions": {
```

```
    "AllocationStrategy": "capacity-optimized-prioritized"
},
"LaunchTemplateConfigs": [
{
    "LaunchTemplateSpecification": {
        "LaunchTemplateName": "my-launch-template",
        "Version": "1"
    },
    "Overrides": [
        {
            "InstanceType": "r4.2xlarge",
            "Priority": 1
            "Placement": {
                "AvailabilityZone": "us-west-2a"
            },
        },
        {
            "InstanceType": "m4.2xlarge",
            "Priority": 2
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            },
        },
        {
            "InstanceType": "c5.2xlarge",
            "Priority": 3
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
},
"TargetCapacitySpecification": {
    "TotalTargetCapacity": 50,
    "DefaultTargetCapacityType": "spot"
}
```

Exemplos de configuração de frota spot

Os exemplos a seguir mostram configurações de execução que você pode usar com o comando [request-spot-fleet](#) para criar uma solicitação de frota spot. Para obter mais informações, consulte [Criar uma solicitação de frota spot \(p. 776\)](#).

Note

Para frota spot, não é possível especificar um ID de interface de rede em uma especificação de execução. Omita o parâmetro `NetworkInterfaceID` na especificação de execução.

Exemplos

- [Exemplo 1: executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço da região \(p. 838\)](#)
- [Exemplo 2: executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço de uma lista especificada \(p. 838\)](#)
- [Exemplo 3: executar Instâncias spot usando o tipo de instância de menor preço de uma lista especificada \(p. 840\)](#)
- [Exemplo 4: Cancelar o preço da solicitação \(p. 841\)](#)
- [Exemplo 5: executar uma frota spot usando a estratégia de alocação diversificada \(p. 842\)](#)
- [Exemplo 6: executar uma frota spot usando o peso da instância \(p. 844\)](#)
- [Exemplo 7: executar uma frota spot com capacidade sob demanda \(p. 845\)](#)

- Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição (p. 846)
- Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade (p. 847)
- Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades (p. 847)

Exemplo 1: executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço da região

O exemplo a seguir determina uma única especificação de execução sem uma zona de disponibilidade nem sub-rede. A frota spot executa as instâncias na zona de disponibilidade de menor preço que tem uma sub-rede padrão. O preço que você paga não excede o preço sob demanda.

```
{  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "KeyName": "my-key-pair",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "m3.medium",  
            "IamInstanceProfile": {  
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
            }  
        }  
    ]  
}
```

Exemplo 2: executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço de uma lista especificada

Os exemplos a seguir determinam duas especificações de execução com zonas de disponibilidade ou sub-redes diferentes, mas o mesmo tipo de instância e AMI.

Zonas de disponibilidade

A frota spot executa as instâncias na sub-rede padrão da zona de disponibilidade de menor preço especificada.

```
{  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "KeyName": "my-key-pair",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "m3.medium",  
            "SubnetIds": ["subnet-12345678"]  
        }  
    ]  
}
```

```
        "Placement": {  
            "AvailabilityZone": "us-west-2a, us-west-2b"  
        },  
        "IamInstanceProfile": {  
            "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
        }  
    }  
}
```

Sub-redes

Você pode especificar sub-redes padrão ou não padrão, e as sub-rede não padrão podem ser de uma VPC padrão ou não padrão. O serviço spot executa as instâncias em qualquer sub-rede na zona de disponibilidade de menor preço.

Você não pode especificar sub-redes diferentes da mesma zona de disponibilidade em uma solicitação de frota spot.

```
{  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "KeyName": "my-key-pair",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "m3.medium",  
            "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",  
            "IamInstanceProfile": {  
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"  
            }  
        }  
    ]  
}
```

Se as instâncias forem executadas em uma VPC padrão, elas receberão um endereço IPv4 público por padrão. Se as instâncias forem executadas em uma VPC não padrão, elas não receberão um endereço IPv4 público por padrão. Use uma interface de rede na especificação de execução para atribuir um endereço IPv4 público às instâncias executadas em uma VPC não padrão. Ao especificar uma interface de rede, você deve incluir o ID da sub-rede e o ID do security group usando a interface de rede.

```
...  
{  
    "ImageId": "ami-1a2b3c4d",  
    "KeyName": "my-key-pair",  
    "InstanceType": "m3.medium",  
    "NetworkInterfaces": [  
        {  
            "DeviceIndex": 0,  
            "SubnetId": "subnet-1a2b3c4d",  
            "Groups": [ "sg-1a2b3c4d" ],  
            "AssociatePublicIpAddress": true  
        }  
    ],  
    "IamInstanceProfile": {  
        "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"  
    }  
}
```

```
    }  
    ...
```

Exemplo 3: executar Instâncias spot usando o tipo de instância de menor preço de uma lista especificada

Os exemplos a seguir determinam duas configurações de execução com tipos de instância diferentes, mas a mesma AMI e zona de disponibilidade ou sub-rede. A frota spot executa as instâncias spot usando o tipo de instância de menor preço especificado.

Availability Zone

```
{  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "cc2.8xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            }  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "r3.8xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            }  
        }  
    ]  
}
```

Sub-rede

```
{  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "cc2.8xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "SecurityGroups": [  
                {  
                    "GroupId": "sg-1a2b3c4d"  
                }  
            ],  
            "InstanceType": "r3.8xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        }  
    ]  
}
```

```
        "SecurityGroups": [
            {
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "InstanceType": "r3.8xlarge",
        "SubnetId": "subnet-1a2b3c4d"
    }
}
```

Exemplo 4. Cancelar o preço da solicitação

Recomendamos que você use o preço máximo padrão, que é o preço sob demanda. Se você preferir, poderá especificar um preço máximo para a solicitação da frota e os preços máximos para as especificações de execução individuais.

Os seguintes exemplos especificam um preço máximo para a solicitação da frota e preços máximos para duas das três especificações de execução. O preço máximo da solicitação da frota é utilizado para qualquer especificação de execução que não especifique um preço máximo. A frota spot executa as instâncias spot usando o tipo de instância de menor preço.

Availability Zone

```
{
    "SpotPrice": "1.00",
    "TargetCapacity": 30,
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            },
            "SpotPrice": "0.10"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.4xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            },
            "SpotPrice": "0.20"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

Sub-rede

```
{
    "SpotPrice": "1.00",
    "TargetCapacity": 30,
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
```

```
"LaunchSpecifications": [
    {
        "ImageId": "ami-1a2b3c4d",
        "InstanceType": "c3.2xlarge",
        "SubnetId": "subnet-1a2b3c4d",
        "SpotPrice": "0.10"
    },
    {
        "ImageId": "ami-1a2b3c4d",
        "InstanceType": "c3.4xlarge",
        "SubnetId": "subnet-1a2b3c4d",
        "SpotPrice": "0.20"
    },
    {
        "ImageId": "ami-1a2b3c4d",
        "InstanceType": "c3.8xlarge",
        "SubnetId": "subnet-1a2b3c4d"
    }
]
```

Exemplo 5: executar uma frota spot usando a estratégia de alocação diversificada

O exemplo a seguir usa a estratégia de alocação diversified. As especificações de execução têm tipos de instância diferentes, mas a mesma AMI e zona de disponibilidade ou sub-rede. A frota spot distribui as 30 instâncias pelas três especificações de execução, de modo que haja 10 instâncias de cada tipo. Para obter mais informações, consulte [Estratégia de alocação para Instâncias spot \(p. 762\)](#).

Availability Zone

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            }
        }
    ]
}
```

Sub-rede

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 30,  
    "AllocationStrategy": "diversified",  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c4.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "m3.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        }  
    ]  
}
```

Para aumentar a chance de que uma solicitação spot possa ser atendida pela capacidade do EC2 no caso de uma interrupção em uma das zonas de disponibilidade, uma prática recomendada é diversificar entre zonas. Nesse cenário, inclua cada zona de disponibilidade possível para você na especificação de execução. E, em vez de usar sempre a mesma sub-rede, use três sub-redes exclusivas (cada mapeamento para uma zona de disponibilidade diferente).

Availability Zone

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 30,  
    "AllocationStrategy": "diversified",  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c4.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2a"  
            }  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "m3.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            }  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2c"  
            }  
        }  
    ]  
}
```

Sub-rede

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 30,  
    "AllocationStrategy": "diversified",  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c4.2xlarge",  
            "SubnetId": "subnet-1a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "m3.2xlarge",  
            "SubnetId": "subnet-2a2b3c4d"  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "SubnetId": "subnet-3a2b3c4d"  
        }  
    ]  
}
```

Exemplo 6: executar uma frota spot usando o peso da instância

Os exemplos a seguir usam o peso da instância, o que significa que o preço é por hora em vez de ser por hora de instância. Cada configuração de execução lista um tipo de instância e um peso diferentes. A frota spot seleciona o tipo de instância com o menor preço por hora de unidade. A frota spot calcula o número de instâncias spot a serem executadas dividindo a capacidade de destino pelo peso da instância. Se o resultado não for um valor inteiro, a frota spot o arredondará para o próximo valor inteiro, para que o tamanho de sua frota não fique abaixo de sua capacidade de destino.

Se a solicitação `r3.2xlarge` for feita com êxito, o spot provisionará 4 dessas instâncias. Divida 20 por 6 para um total de 3,33 instâncias, em seguida, arredonde para 4 instâncias.

Se a solicitação `c3.xlarge` for feita com êxito, o spot provisionará 7 dessas instâncias. Divida 20 por 3 para um total de 6,66 instâncias, em seguida, arredonde para 7 instâncias.

Para obter mais informações, consulte [Peso de instâncias de frotas spot \(p. 768\)](#).

Availability Zone

```
{  
    "SpotPrice": "0.70",  
    "TargetCapacity": 20,  
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",  
    "LaunchSpecifications": [  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "r3.2xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            },  
            "WeightedCapacity": 6  
        },  
        {  
            "ImageId": "ami-1a2b3c4d",  
            "InstanceType": "c3.xlarge",  
            "Placement": {  
                "AvailabilityZone": "us-west-2b"  
            },  
            "WeightedCapacity": 14  
        }  
    ]  
}
```

```
        "WeightedCapacity": 3
    }
}
```

Sub-rede

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 20,
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "WeightedCapacity": 6
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "WeightedCapacity": 3
        }
    ]
}
```

Exemplo 7: executar uma frota spot com capacidade sob demanda

Para garantir que você sempre tenha capacidade de instância, você pode incluir uma solicitação de capacidade sob demanda na solicitação de frota spot. Se houver capacidade, a solicitação de sob demanda sempre será atendida. O equilíbrio da capacidade de destino será atendido como Spot se houver capacidade e disponibilidade.

O exemplo a seguir especifica a capacidade desejada de destino como 10, da qual 5 deve ser sob demanda. A capacidade spot não é especificada. Ela está implícita no saldo da capacidade pretendida menos a capacidade sob demanda. O Amazon EC2 executará cinco unidades de capacidade como sob demanda e cinco unidades de capacidade ($10-5=5$) como spot se houver disponibilidade e capacidade do Amazon EC2 disponíveis.

Para obter mais informações, consulte [Sob demanda na frota spot \(p. 765\)](#).

```
{
    "IamFleetRole": "arn:aws:iam::781603563322:role/aws-ec2-spot-fleet-tagging-role",
    "AllocationStrategy": "lowestPrice",
    "TargetCapacity": 10,
    "SpotPrice": null,
    "ValidFrom": "2018-04-04T15:58:13Z",
    "ValidUntil": "2019-04-04T15:58:13Z",
    "TerminateInstancesWithExpiration": true,
    "LaunchSpecifications": [],
    "Type": "maintain",
    "OnDemandTargetCapacity": 5,
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0ddb04d4a6cca5ad1",
                "Version": "2"
            }
        }
    ]
}
```

```
"Overrides": [
    {
        "InstanceType": "t2.medium",
        "WeightedCapacity": 1,
        "SubnetId": "subnet-d0dc51fb"
    }
]
```

Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição

O exemplo a seguir configura a frota spot para executar uma instância spot de substituição quando o Amazon EC2 emite uma recomendação de rebalanceamento para uma instância spot na frota. Para configurar a substituição automática da Instâncias spot, para `ReplacementStrategy`, especifique `launch`.

Note

Quando uma instância de substituição é executada, a instância marcada para rebalanceamento não é automaticamente encerrada. Você pode encerrá-la, ou você pode deixá-la em funcionamento. Você é cobrado por ambas as instâncias enquanto elas estão sendo executadas.

A eficácia da estratégia de rebalanceamento de capacidade depende do número de grupos de capacidade spot especificados na solicitação de frota spot. Recomendamos que você configure a frota com um conjunto diversificado de tipos de instância e zonas de disponibilidade e para `AllocationStrategy` especifique `capacityOptimized`. Para obter mais informações sobre o que você deve considerar ao configurar uma frota spot para rebalanceamento de capacidade, consulte [Rebalanceamento de capacidade \(p. 765\)](#).

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                    {
                        "InstanceType": "c3.large",
                        "WeightedCapacity": 1,
                        "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    },
                    {
                        "InstanceType": "c4.large",
                        "WeightedCapacity": 1,
                        "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    },
                    {
                        "InstanceType": "c5.large",
                        "WeightedCapacity": 1,
                        "Placement": {
                            "AvailabilityZone": "us-east-1a"
                        }
                    }
                ]
            }
        ]
    }
}
```

```
        "AvailabilityZone": "us-east-1a"
    }
}
],
"TargetCapacity": 5,
"SpotMaintenanceStrategies": {
    "CapacityRebalance": {
        "ReplacementStrategy": "launch"
    }
}
}
```

Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade

O exemplo a seguir demonstra como configurar uma frota spot com uma estratégia de alocação spot que otimiza a capacidade. Para otimizar a capacidade, você deve definir AllocationStrategy como capacityOptimized.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. A capacidade pretendida é de 50 Instâncias spot. A frota spot tenta iniciar 50 instâncias spot no grupo de capacidade spot com a capacidade ideal para o número de instâncias em execução.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                    "AvailabilityZone": "us-west-2a"
                },
                {
                    "InstanceType": "m4.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                },
                {
                    "InstanceType": "c5.2xlarge",
                    "AvailabilityZone": "us-west-2b"
                }
            ]
        }
    ]
}
```

Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades

O exemplo a seguir demonstra como configurar uma frota spot com uma estratégia de alocação spot que optimiza a capacidade enquanto usa a prioridade com base no melhor esforço.

Ao usar a estratégia de alocação `capacityOptimizedPrioritized`, você pode usar o parâmetro `Priority` para especificar as prioridades dos grupos de capacidade spot, em que quanto menor o número, maior a prioridade. Você também pode definir a mesma prioridade para vários grupos de capacidade spot se você favorecê-los igualmente. Se você não definir uma prioridade para um grupo, ele será considerado o último em termos de prioridade.

Para priorizar grupos de capacidade spot, você deve definir `AllocationStrategy` como `capacityOptimizedPrioritized`. A frota spot otimizará a capacidade em primeiro lugar, mas honrará as prioridades com o melhor esforço (por exemplo, se honrar as prioridades não afetará significativamente a capacidade da frota spot de provisionar a capacidade ideal). Essa é uma boa opção para workloads em que a possibilidade de interrupção deve ser minimizada e a preferência por determinados tipos de instância for importante.

No exemplo a seguir, as três especificações de lançamento especificam três grupos de capacidade spot. Cada grupo é priorizado, onde quanto menor o número, maior a prioridade. A capacidade pretendida é de 50 Instâncias spot. A frota spot tenta executar 50 instâncias Spot no grupo de capacidade spot com a maior prioridade com base no melhor esforço, mas otimiza a capacidade em primeiro lugar.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "r4.2xlarge",
                    "PriorityPriorityPriority
```

Quotas da frota

As cotas normais do Amazon EC2 se aplicam a instâncias executadas por uma EC2 Fleet ou uma frota spot, como [limites de instância spot \(p. 347\)](#) e [limites de volume \(p. 1507\)](#). Além disso, os limites a seguir são aplicáveis:

- O número de frotas spot e frotas do EC2 ativas por região: 1.000* †
- O número de grupos de capacidade spot (combinação exclusiva de tipo de instância e sub-rede): 300* ‡
- O tamanho dos dados de usuário em uma especificação de execução: 16 KB †

- A capacidade pretendida por EC2 Fleet ou frota spot: 10.000
- A capacidade de destino em todas as Frotas do EC2 e Frotas spot de uma região: 100.000*
- Uma solicitação de EC2 Fleet ou de frota spot não pode abranger regiões.
- Uma solicitação de EC2 Fleet ou de frota spot não pode abranger sub-redes diferentes na mesma zona de disponibilidade.

*Esses limites aplicam-se à Frotas do EC2 e Frotas spot.

† Esses são limites fixos. Não é possível solicitar um aumento de limite para eles.

‡ Esse limite só se aplica a frotas de tipo `request` ou `maintain`. Esse limite não se aplica a frotas `instant`.

Para solicitar um aumento de limite para a capacidade pretendida

Se você precisar exceder os limites padrão da capacidade de destino, preencha o formulário [Create case](#) (Criar caso) do AWS Support Center para solicitar um aumento de limite. Para Limit type (Tipo de limite), selecione EC2 Fleet (Frota do EC2), selecione uma região e depois selecione Target Fleet Capacity per Fleet (in units) (Capacidade da frota de destino por frota (em unidades)) ou Target Fleet Capacity per Region (in units) (Capacidade da frota de destino por região (em unidades)) ou ambas as opções.

Amazon Elastic Graphics

O Amazon Elastic Graphics oferece aceleração gráfica flexível, de baixo custo e de alta performance para suas instâncias do Windows. As aceleradoras do Elastic Graphics são fornecidas em vários tamanhos e são uma alternativa de baixo custo para usar tipos de instâncias de gráficos de GPU (como G2 e G3). Você tem a flexibilidade de escolher um tipo de instância que atenda às necessidades de computação, memória e armazenamento de sua aplicação. Em seguida, escolha o acelerador para sua instância que atenda aos requisitos gráficos de sua workload.

O Elastic Graphics é adequado para aplicações que exigem uma quantidade pequena ou intermitente de aceleração gráfica adicional e que usam o suporte gráfico OpenGL. Se você precisa de acesso a GPUs completas e anexadas diretamente e precisa usar frameworks de computação paralela DirectX, CUDA ou Open Computing Language (OpenCL), use um tipo de instância de computação acelerada. Para obter mais informações, consulte [Windows Instâncias computacionais aceleradas](#) (p. 228).

Tópicos

- [Conceitos básicos de Elastic Graphics](#) (p. 850)
- [Definição de preço do Elastic Graphics](#) (p. 852)
- [Limitações de Elastic Graphics](#) (p. 852)
- [Como trabalhar com o Elastic Graphics](#) (p. 852)
- [Usar métricas do CloudWatch para monitorar o Elastic Graphics](#) (p. 858)
- [Troubleshoot](#) (p. 860)

Conceitos básicos de Elastic Graphics

Para usar o Elastic Graphics, execute uma instância do Windows e especifique um tipo de aceleradora para a instância durante a execução. A AWS encontra a capacidade disponível para o Elastic Graphics e estabelece uma conexão de rede entre a instância e a aceleradora do Elastic Graphics.

Note

Não há suporte para instâncias bare metal

As aceleradoras do Elastic Graphics estão disponíveis nas seguintes regiões da AWS: `us-east-1`, `us-east-2`, `us-west-2`, `ap-northeast-1`, `ap-southeast-1`, `ap-southeast-2`, `eu-central-1` e `eu-west-1`.

Os tipos de instância a seguir oferecem suporte a aceleradores do Elastic Graphics:

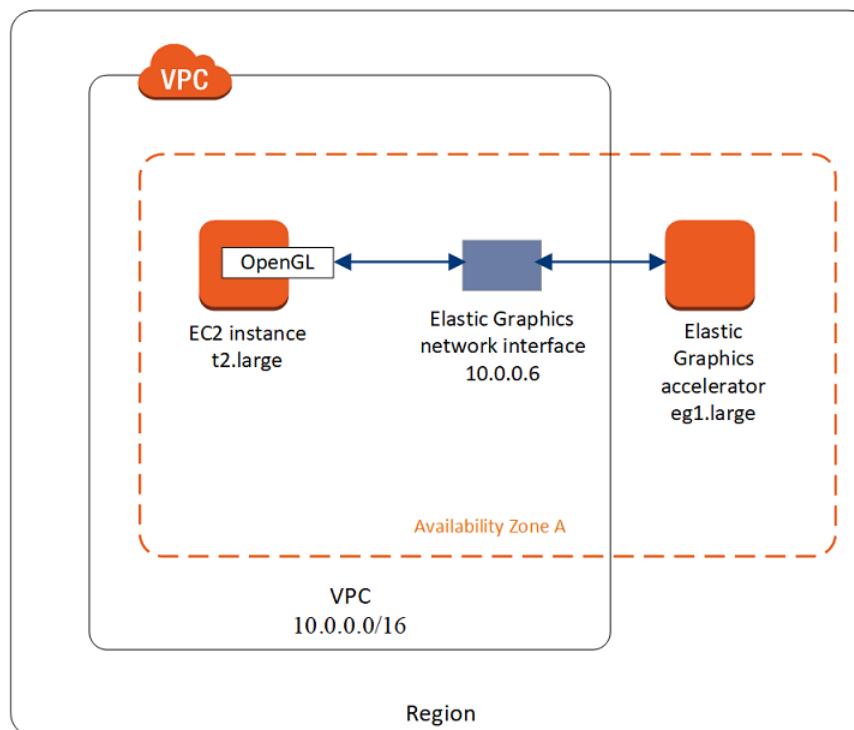
- C3 | C4 | C5 | C5a | C5ad | C5d | C5n
- D2 | D3 | D3en
- H1
- I3 | I3en
- M3 | M4 | M5 | M5d | M5dn | M5n
- P2 | P3 | P3dn
- R3 | R4 | R5 | R5d | R5dn | R5n
- `t2.medium` ou maior | `t3.medium` ou maior
- X1 | X1e
- z1d

O aceleradores do Elastic Graphics a seguir estão disponíveis. Você pode anexar qualquer acelerador do Elastic Graphics a qualquer tipo de instância compatível.

Aceleradora do Elastic Graphics	Memória gráfica (GB)
eg1.medium	1
eg1.large	2
eg1.xlarge	4
eg1.2xlarge	8

Um acelerador do Elastic Graphics não faz parte do hardware de sua instância. Em vez disso, ele é anexado à rede por meio de uma interface de rede, conhecida como a interface de rede do Elastic Graphics. Ao executar ou reiniciar uma instância com aceleração gráfica, a interface de rede do Elastic Graphics é criada em sua VPC.

A interface de rede do Elastic Graphics é criada nas mesmas sub-rede e VPC de sua instância e recebe um IPv4 privado dessa sub-rede. O acelerador anexado a sua instância do Amazon EC2 é alocado a partir de um grupo de aceleradores disponíveis na mesma zona de disponibilidade de sua instância.



Os aceleradores do Elastic Graphics oferecem suporte aos padrões da API do OpenGL 4.3 e anteriores, que podem ser usados para aplicações em lotes ou para aceleração gráfica em 3D. Uma biblioteca do OpenGL otimizada pela Amazon em sua instância detecta o acelerador anexado. Ela direciona as chamadas à OpenGL API de sua instância para o acelerador, que, em seguida, processa as solicitações e retorna os resultados. O tráfego entre a instância e o acelerador usa a mesma largura de banda que o tráfego de rede da instância, portanto, recomendamos que você tenha largura de banda de rede adequada disponível. Consulte seu fornecedor de software em relação a dúvidas sobre conformidade e versão do OpenGL.

Como padrão, o grupo de segurança padrão de sua VPC é associado à interface de rede do Elastic Graphics. O tráfego de rede do Elastic Graphics usa o protocolo TCP e a porta 2007. Certifique-se de que o security group de sua instância permita isso. Para obter mais informações, consulte [Configurar grupos de segurança \(p. 853\)](#).

Definição de preço do Elastic Graphics

Você será cobrado por cada segundo em que um acelerador do Elastic Graphics estiver anexado a uma instância no estado `running` quando o acelerador estiver no estado `Ok`. Você não é cobrado por um acelerador anexado a uma instância que esteja no estado `pending`, `stopping`, `stopped`, `shutting-down` ou `terminated`. Você também não é cobrado quando um acelerador estiver no estado `Unknown` ou `Impaired`.

A definição de preço de aceleradores está disponível apenas a taxas sob demanda. Você pode anexar um aceleradora a uma instância reservada ou instância spot, no entanto, o preço sob demanda da aceleradora se aplica.

Para obter mais informações, consulte [Definição de preço Amazon Elastic Graphics](#).

Limitações de Elastic Graphics

Antes de começar a usar aceleradores do Elastic Graphics, esteja ciente das seguintes limitações:

- Só é possível anexar aceleradores a instâncias do Windows com o Microsoft Windows Server 2012 R2 ou posterior. No momento, não há suporte às instâncias do Linux.
- É possível anexar uma aceleradora por vez a uma instância.
- É possível anexar apenas uma aceleradora durante o lançamento da instância. Não é possível anexar uma aceleradora a uma instância existente.
- Você não pode hibernar uma instância com uma aceleradora anexada.
- Não é possível compartilhar um acelerador entre instâncias.
- Não é possível desanexar um acelerador de uma instância ou transferi-lo para outra instância. Se você não precisar mais de um acelerador, será necessário encerrar a instância. Para alterar o tipo de acelerador, crie uma AMI a partir de sua instância, encerre-a e execute uma nova instância com uma especificação de acelerador diferente.
- As únicas versões compatíveis da OpenGL API são a 4.3 e anteriores. DirectX, CUDA, e OpenCL não são compatíveis.
- O acelerador do Elastic Graphics não é visível ou acessível por meio do gerenciador de dispositivos de sua instância.
- Você não pode reservar ou programar capacidade para o acelerador.
- Você não pode anexar aceleradores a instâncias no EC2-Classic.
- Você não pode anexar aceleradores a instâncias configuradas para usar o Instance Metadata Service v2 (IMDSv2).

Como trabalhar com o Elastic Graphics

Você pode executar uma instância e associá-la a um acelerador do Elastic Graphics durante a execução. Em seguida, você deve instalar as bibliotecas necessárias manualmente em sua instância que permitam a comunicação com o acelerador. Para obter limitações, consulte [Limitações de Elastic Graphics \(p. 852\)](#).

Tarefas

- [Configurar grupos de segurança \(p. 853\)](#)
- [Iniciar uma instância com uma aceleradora do Elastic Graphics \(p. 854\)](#)
- [Instalar o software necessário para o Elastic Graphics \(p. 855\)](#)
- [Verificar a funcionalidade do Elastic Graphics em sua instância \(p. 855\)](#)
- [Ver informações do Elastic Graphics \(p. 857\)](#)
- [Enviar feedback \(p. 858\)](#)

Configurar grupos de segurança

O Elastic Graphics requer um grupo de segurança de autorreferência que permita todo o tráfego de entrada e saída do grupo de segurança e para ele próprio. O grupo de segurança deve incluir as seguintes regras de entrada e saída:

Regra de entrada			
Type	Protocolo	Port	Origem
Elastic Graphics	TCP	2007	O ID do grupo de segurança (seu próprio ID de recurso)
Regra de saída			
Type	Protocolo	Port Range (Intervalo de portas)	Destino
Elastic Graphics	TCP	2007	O ID do grupo de segurança (seu próprio ID de recurso)

Ao usar o console do Amazon EC2 para iniciar sua instância com um acelerador do Elastic Graphics, você poderá permitir que o assistente de execução crie automaticamente as regras do grupo de segurança necessárias ou selecione uma segurança criada anteriormente.

Se você estiver iniciando sua instância usando a AWS CLI ou um SDK, será necessário especificar um grupo de segurança criado anteriormente.

Para criar um grupo de segurança para o Elastic Graphics

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Security Groups (Grupos de segurança) e, em seguida, Create Security Group (Criar grupo de segurança).
3. Na janela Security group (Grupo de segurança), faça o seguinte:
 - a. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança, como **Elastic Graphics security group**.
 - b. (Opcional) Em Description (Descrição), insira uma breve descrição do grupo de segurança.
 - c. Em VPC, selecione a VPC na qual você pretende usar o Elastic Graphics.
 - d. Escolha Create security group (Criar grupo de segurança).
4. No painel de navegação, escolha Security Groups (Grupos de segurança), selecione o grupo de segurança que você acabou de criar e na guia Details (Detalhes), copie o ID do grupo de segurança.
5. Na guia Inbound rules (Regras de entrada), escolha Edit inbound rules (Editar regras de entrada) e faça o seguinte:

- a. Escolha Add rule (Adicionar regra).
 - b. Em Type (Tipo), escolha Elastic Graphics.
 - c. Em Source type (Tipo de origem), escolha Custom (Personalizado).
 - d. Em Source (Origem), cole o ID do grupo de segurança que copiou anteriormente.
 - e. Escolha Salvar regras.
6. Na guia Outbound rules (Regras de saída), escolha Edit outbound rules (Editar regras de saída) e faça o seguinte:
 - a. Escolha Add rule (Adicionar regra).
 - b. Em Type (Tipo), escolha Elastic Graphics.
 - c. Em Destination type (Tipo de destino), escolha Custom (Personalizado).
 - d. Em Destination (Destino), cole o ID do grupo de segurança que copiou anteriormente.
 - e. Escolha Salvar regras.

Para obter mais informações, consulte [Grupos de segurança do Amazon EC2 para instâncias do Windows \(p. 1217\)](#).

Iniciar uma instância com uma aceleradora do Elastic Graphics

É possível associar um acelerador do Elastic Graphics a uma instância durante a execução. Se houver falha na execução, os seguintes motivos serão possíveis:

- Capacidade insuficiente do acelerador do Elastic Graphics
- Limite excedido nos aceleradores do Elastic Graphics na região
- Não há endereços IPv4 privados suficientes em sua VPC para criar uma interface de rede para o acelerador

Para obter mais informações, consulte [Limitações de Elastic Graphics \(p. 852\)](#).

Para associar um acelerador do Elastic Graphics durante a execução da instância (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel, escolha Launch Instance (Executar instância).
3. Selecione a AMI do Windows e um tipo de instância compatível. Para obter mais informações, consulte [Conceitos básicos de Elastic Graphics \(p. 850\)](#).
4. Na página Configure Instance Details, selecione uma VPC e uma sub-rede em que sua instância será executada.
5. Escolha Add Graphics Acceleration (Adicionar aceleração gráfica) e selecione um tipo de acelerador do Elastic Graphics.
6. (Opcional) Nas páginas Add Storage (Adicionar armazenamento) e Add Tags (Adicionar tags), adicione os volumes e as tags necessárias.
7. Na página Configure Security Group (Configurar o grupo de segurança), você pode deixar o console criar um grupo de segurança para você com as regras de entrada e de saída necessárias ou usar o grupo de segurança criado manualmente em [Configurar grupos de segurança \(p. 853\)](#). Adicione grupos de segurança adicionais conforme necessário.
8. Escolha Review and Launch (Revisar e executar) para revisar as opções da instância e escolha Launch (Executar).

Para associar uma aceleradora do Elastic Graphics durante a execução da instância (AWS CLI)

Você pode usar o comando [run-instances](#) da AWS CLI com o seguinte parâmetro:

```
--elastic-gpu-specification Type=eg1.medium
```

Para o parâmetro --security-group-ids, você deve incluir um grupo de segurança que tenha as regras de entrada e saída necessárias. Para obter mais informações, consulte [Configurar grupos de segurança \(p. 853\)](#).

Para associar um acelerador do Elastic Graphics durante a execução da instância (Tools for Windows PowerShell).

Use o comando [New-EC2Instance](#) do Tools for Windows PowerShell.

Instalar o software necessário para o Elastic Graphics

Se você tiver executado a instância usando uma AMI Do Windows para AWS, o software necessário será instalado automaticamente durante a primeira inicialização. Se tiver executado a instância usando AMIs do Windows que não instalam o software necessário automaticamente, você deverá instalar o software necessário na instância manualmente.

Para instalar o software necessário para o Elastic Graphics (se necessário)

1. Conecte-se à instância.
2. Faça download do [Instalador do Elastic Graphics](#) e abra-o. O gerenciador de instalação conecta-se ao endpoint do Elastic Graphics e faz download da versão mais recente do software necessário.
3. Reinicie a instância para verificar.

Verificar a funcionalidade do Elastic Graphics em sua instância

Os pacotes do Elastic Graphics em sua instância incluem ferramentas que você pode usar para visualizar o status do acelerador e verificar se os comandos do OpenGL de sua instância para o acelerador estão funcionais.

Se sua instância foi executada com uma AMI que não tenha os pacotes do Elastic Graphics pré-instalados, você mesmo poderá fazer download e instalá-los. Para obter mais informações, consulte [Instalar o software necessário para o Elastic Graphics \(p. 855\)](#).

Tópicos

- [Usar o monitor de status do Elastic Graphics \(p. 855\)](#)
- [Usar a ferramenta da linha de comando do Elastic Graphics \(p. 856\)](#)

Usar o monitor de status do Elastic Graphics

Você pode usar a ferramenta de monitor de status para visualizar informações sobre o status de um acelerador do Elastic Graphics. Por padrão, essa ferramenta está disponível na área de notificação da barra de tarefas em sua instância do Windows e mostra o status do acelerador gráfico. Os valores possíveis são os seguintes.

Integridade

O acelerador do Elastic Graphics está habilitado e íntegro.

Atualizando

O status do acelerador do Elastic Graphics é em atualização no momento. Pode levar alguns minutos para que o status seja exibido.

Fora de serviço

O acelerador do Elastic Graphics está fora de serviço. Para obter mais informações sobre o erro, escolha Read More (Leia mais).

Usar a ferramenta da linha de comando do Elastic Graphics

É possível usar a ferramenta de linha de comando do Elastic Graphics, `egcli.exe`, para verificar o status do acelerador. Se houver um problema com o acelerador, a ferramenta retornará uma mensagem de erro.

Para executar a ferramenta, abra um prompt de comando em sua instância e execute o seguinte comando:

```
C:\Program Files\Amazon\EC2ElasticGPUs\manager\egcli.exe
```

A ferramenta também oferece suporte aos seguintes parâmetros:

`--json, -j`

Indica se a mensagem JSON deve ser mostrada. Os valores possíveis são `true` e `false`. O padrão é `true`.

`--imds, -i`

Indica se os metadados da instância devem ser verificados para ver a disponibilidade do acelerador. Os valores possíveis são `true` e `false`. O padrão é `true`.

A seguir está um exemplo de saída. O status de `OK` indica que o acelerador está habilitado e íntegro.

```
EG Infrastructure is available.  
Instance ID egpu-f6d94dfa66df4883b284e96db7397ee6  
Instance Type eg1.large  
EG Version 1.0.0.885 (Manager) / 1.0.0.95 (OpenGL Library) / 1.0.0.69 (OpenGL Redirector)  
EG Status: Healthy  
JSON Message:  
{  
    "version": "2016-11-30",  
    "status": "OK"  
}
```

Os valores possíveis para são os seguinte `status`:

`OK`

O acelerador do Elastic Graphics está habilitado e íntegro.

`UPDATING`

O driver do Elastic Graphics está sendo atualizado.

`NEEDS_REBOOT`

O driver do Elastic Graphics foi atualizado e uma reinicialização da instância do Amazon EC2 é necessária.

LOADING_DRIVER

O driver do Elastic Graphics está sendo carregado.

CONNECTING_EGPU

O driver do Elastic Graphics está verificando a conectividade com o acelerador do Elastic Graphics.

ERROR_UPDATE_RETRY

Ocorreu um erro ao atualizar o driver do Elastic Graphics, uma atualização será tentada novamente em breve.

ERROR_UPDATE

Ocorreu um erro irrecuperável ao atualizar o driver do Elastic Graphics.

ERROR_LOAD_DRIVER

Ocorreu um erro ao carregar o driver do Elastic Graphics.

ERROR_EGPU_CONNECTIVITY

O acelerador do Elastic Graphics está inacessível.

Ver informações do Elastic Graphics

É possível visualizar as informações sobre o acelerador do Elastic Graphics anexado a sua instância.

Para visualizar informações sobre um acelerador do Elastic Graphics (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. Na guia Details (Detalhes) , localize o Elastic Graphics ID (ID do Elastic Graphics). Escolha o ID para visualizar as seguintes informações sobre o acelerador do Elastic Graphics:
 - Attachment State (Estado do anexo)
 - Type
 - Health status (Status da integridade)

Para visualizar informações sobre uma aceleradora do Elastic Graphics (AWS CLI)

Você pode usar o comando da AWS CLI [describe-elastic-gpus](#):

```
aws ec2 describe-elastic-gpus
```

Você pode usar o comando [describe-network-interfaces](#) da AWS CLI e filtrar por ID de proprietário para visualizar informações sobre a interface de rede do Elastic Graphics.

```
aws ec2 describe-network-interfaces --filters "Name=attachment.instance-owner-id,Values=amazon-elasticgpus"
```

Para visualizar informações sobre um acelerador do Elastic Graphics (Tools for Windows PowerShell)

Use os seguintes comandos:

- [Get-EC2ElasticGpu](#)
- [Get-EC2NetworkInterface](#)

Para visualizar informações sobre um acelerador do Elastic Graphics usando metadados da instância

1. Conecte-se à instância do Windows que está usando um acelerador do Elastic Graphics.
2. Execute um destes procedimentos:
 - No PowerShell, use o seguinte cmdlet:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
```

- No navegador da Web, cole a seguinte URL no campo de endereço:

```
http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
```

Enviar feedback

Nas etapas a seguir, você pode enviar comentários sobre sua experiência com o Elastic Graphics para que a equipe possa fazer melhorias adicionais.

Para enviar comentários usando o monitor de status do Elastic Graphics

1. Na área de notificação da barra de tarefas da instância do Windows, abra o monitor de status do Elastic Graphics.
2. No canto inferior esquerdo, escolha Feedback (Comentários).
3. Digite seus comentários e selecione Submit.

Usar métricas do CloudWatch para monitorar o Elastic Graphics

É possível monitorar o acelerador do Elastic Graphics usando o Amazon CloudWatch, que coleta métricas sobre a performance do acelerador. Essas estatísticas são registradas por um período de duas semanas, para que você possa acessar informações históricas e obter uma perspectiva melhor sobre a performance de seu serviço.

Por padrão, os aceleradores do Elastic Graphics enviam dados de métricas ao CloudWatch em períodos de 5 minutos.

Para obter mais informações sobre o Amazon CloudWatch, consulte o [Guia do usuário do Amazon CloudWatch](#).

Métricas do Elastic Graphics

O namespace AWS/ElasticGPUs inclui as seguintes métricas para o Elastic Graphics.

Métrica	Descrição
GPUConnectivityCheckFailed	Informa se a conectividade com o acelerador do Elastic Graphics está ativa ou falhou. Um valor de zero (0) indica que a conexão está ativa. Um valor de um (1) uma falha de conectividade.

Métrica	Descrição
	Unidades: contagem
GPUHealthCheckFailed	Informa se o acelerador do Elastic Graphics foi aprovado na verificação de integridade de status no último minuto. Um valor de zero (0) indica que a verificação de status obteve aprovação. Um valor de um (1) uma falha na verificação de status. Unidades: contagem
GPUMemoryUtilization	A memória da GPU usada. Unidades: MiB

Dimensões do Elastic Graphics

Você pode filtrar os dados de métricas de seus aceleradores do Elastic Graphics usando as seguintes dimensões.

Dimensão	Descrição
EGPUId	Filtre os dados pelo acelerador do Elastic Graphics.
InstanceId	Filtre os dados pela instância à qual o acelerador do Elastic Graphics está anexado.

Visualizar métricas do CloudWatch para o Elastic Graphics

As métricas são agrupadas primeiro pelo namespace do serviço e, em seguida, pelas várias dimensões com suporte. Você pode usar os procedimentos a seguir para visualizar as métricas dos aceleradores do Elastic Graphics.

Para visualizar as métricas do Elastic Graphics no console do CloudWatch

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. Se necessário, altere a região. Na barra de navegação, selecione a região em que o acelerador do Elastic Graphics reside. Para obter mais informações, consulte [Regiões e endpoints](#).
3. No painel de navegação, selecione Metrics (Métricas).
4. Em All metrics (Todas as métricas), selecione Elastic Graphics, Elastic Graphics Metrics (Métricas do Elastic Graphics).

Para visualizar métricas do Elastic Graphics (AWS CLI)

Use o comando [list-metrics](#) a seguir:

```
aws cloudwatch list-metrics --namespace "AWS/ElasticGPUs"
```

Criar alarmes do CloudWatch para monitorar o Elastic Graphics

Você pode criar um alarme do CloudWatch que envia uma mensagem de Amazon SNS quando o alarme mudar de estado. Um alarme observa uma única métrica por um período especificado por você e envia uma notificação para um tópico do Amazon SNS com base no valor da métrica em relação a determinado limite ao longo de vários períodos.

Por exemplo, é possível criar um alarme que monitore a integridade de um acelerador do Elastic Graphics e envie uma notificação quando ocorrer uma falha na verificação de integridade do acelerador gráfico por três períodos consecutivos de cinco minutos.

Para criar um alarme para o status de integridade de um acelerador do Elastic Graphics

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, escolha Alarms, Create Alarm.
3. Escolha Select metric (Selecionar métrica), Elastic Graphics, Elastic Graphics Metrics (Métricas do Elastic Graphics).
4. Selecione a métrica GPUHealthCheckFailed e escolha Select metric (Selecionar métrica).
5. Configure o alarme desta forma:
 - a. Em Alarm details (Detalhes do alarme), digite um nome e uma descrição para o alarme. Em Whenever (Sempre), escolha \geq e digite 1.
 - b. Em Actions (Ações), selecione uma lista de notificações existente ou escolha New list (Nova lista).
 - c. Escolha Create Alarm.

Troubleshoot

Veja a seguir erros comuns e etapas de solução de problemas.

Sumário

- [Investigar problemas na performance da aplicação \(p. 860\)](#)
 - Problemas de performance na renderização do OpenGL (p. 861)
 - Problemas na performance do acesso remoto (p. 862)
- [Resolver problemas de status não íntegros \(p. 862\)](#)
 - Interromper e iniciar a instância (p. 862)
 - Verificar os componentes instalados (p. 862)
 - Verificar os logs do Elastic Graphics (p. 862)

Investigar problemas na performance da aplicação

O Elastic Graphics usa a rede de instâncias para enviar comandos OpenGL a uma placa gráfica remotamente anexada. Além disso, um desktop que executa uma aplicação OpenGL com um acelerador do Elastic Graphics geralmente é acessado usando uma tecnologia de acesso remoto. É importante distinguir entre um problema de performance relativo à renderização do OpenGL ou à tecnologia de acesso remoto da área de trabalho.

Problemas de performance na renderização do OpenGL

A performance da renderização do OpenGL é determinada pelo número de comandos e quadros do OpenGL gerados na instância remota.

A performance da renderização pode variar dependendo dos seguintes fatores:

- Performance do acelerador do Elastic Graphics
- Desempenho das redes
- Performance da CPU
- Modelo de renderização, complexidade do cenário
- Comportamento da aplicação OpenGL

Uma maneira fácil de avaliar a performance é exibir o número de quadros renderizados na instância remota. As aceleradoras do Elastic Graphics exibem um máximo de 25 quadros por segundo na instância remota para obter a melhor qualidade percebida e, ao mesmo tempo, reduzir o uso da rede.

Para mostrar o número de quadros produzidos

1. Abra o arquivo a seguir em um editor de texto. Se o arquivo não existir, crie-o.

```
C:\Program Files\Amazon\EC2ElasticGPUs\conf\eg.conf
```

2. Identifique a seção [Application], ou adicione-a se não estiver presente, e adicione o seguinte parâmetros de configuração:

```
[Application]
show_fps=1
```

3. Reinicie a aplicação e verifique o FPS novamente.

Se os quadros/s atingirem 15 a 25 quadros/s ao atualizar a cena renderizada, o acelerador do Elastic Graphics estará executando em pico. Qualquer outro problema de performance percebido provavelmente estará relacionado ao acesso remoto no computador da instância. Se esse for o caso, consulte a seção Problemas de performance do acesso remoto.

Se o número de FPS for menor que 15, você pode testar o seguinte:

- Melhore a performance do acelerador do Elastic Graphics selecionando um tipo de acelerador gráfico mais potente.
- Melhore a performance geral da rede usando estas dicas:
 - Verifique a quantidade de largura de banda de entrada e de saída do endpoint do acelerador do Elastic Graphics. O endpoint do acelerador do Elastic Graphics pode ser recuperado com o seguinte comando do PowerShell:

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/meta-data/elastic-gpus/
associations/[ELASTICGPU_ID]).content
```

- O tráfego de rede da instância para o endpoint do acelerador do Elastic Graphics é relacionado ao volume de comandos que a aplicação OpenGL está produzindo.
- O tráfego de rede do endpoint do acelerador do Elastic Graphics para a instância está relacionado ao número de quadros gerados pelo acelerador gráfico.
- Caso perceba que o uso da rede está alcançando a taxa de dados máxima da rede para as instâncias, tente usar uma instância com uma variação maior na taxa de dados da rede.
- Melhore a performance da CPU:

- As aplicações podem exigir muitos recursos da CPU além do que o acelerador do Elastic Graphics precisa. Se o Gerenciador de Tarefas do Windows estiver informando um uso elevado dos recursos da CPU, tente usar uma instância com mais potência de CPU.

Problemas na performance do acesso remoto

Uma instância com um acelerador do Elastic Graphics anexado pode ser acessada usando diferentes tecnologias de acesso remoto. A performance e a qualidade podem variar dependendo:

- Da tecnologia de acesso remoto
- Do desempenho da instância
- Performance do cliente
- Latência e largura de banda de rede entre o cliente e a instância

Possíveis opções para o protocolo de acesso remoto incluem:

- Conexão de área de trabalho remota da Microsoft
- NICE DCV
- VNC

Para obter mais informações sobre otimização, consulte o protocolo específico.

Resolver problemas de status não íntegros

Se o acelerador do Elastic Graphics estiver em um estado não íntegro, use as etapas de solução de problemas a seguir para resolver o problema.

Interromper e iniciar a instância

Se o acelerador do Elastic Graphics estiver em um estado não íntegro, parar a instância e reiniciá-la é a opção mais simples. Para obter mais informações, consulte [Interromper e iniciar suas instâncias \(p. 457\)](#).

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Verificar os componentes instalados

Abra o Painel de Controle do Windows e confirme se os seguintes componentes estão instalados:

- Gerenciador do Amazon Elastic Graphics
- Biblioteca de OpenGL do Amazon Elastic Graphics
- Redirecionador de OpenGL para GPUs elásticas do Amazon EC2

Se qualquer um desses itens estiver ausente, você deve instalá-lo manualmente. Para obter mais informações, consulte [Instalar o software necessário para o Elastic Graphics \(p. 855\)](#).

Verificar os logs do Elastic Graphics

Abra o Visualizador de eventos do Windows, expanda a seção Application and Services Logs (Logs de aplicações e de serviços) e pesquise por erros nos seguintes logs de eventos:

- EC2ElasticGPUs
- GUI do EC2ElasticGPUs

Monitorar o Amazon EC2

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e a performance de suas instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e de outras soluções da AWS. Você deve coletar dados de monitoramento de todas as partes de suas soluções da AWS para facilitar a depuração de uma falha de vários pontos (caso ocorra). No entanto, antes de iniciar o monitoramento do Amazon EC2, você deve criar um plano de monitoramento que deverá incluir:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

Depois de definir seus objetivos de monitoramento e criar seu plano de monitoramento, a próxima etapa é estabelecer uma linha de base para a performance normal do Amazon EC2 em seu ambiente. Você deve medir a performance do Amazon EC2 em vários momentos e em condições diferentes de carga. Ao monitorar o Amazon EC2, você deve armazenar um histórico dos dados de monitoramento que você reúne. Você poderá comparar a performance atual do Amazon EC2 com esses dados históricos para ajudá-lo a identificar padrões de performance normais e anomalias de performance, e elaborar métodos para resolvê-los. Por exemplo, é possível monitorar a utilização da CPU, a E/S de disco e a utilização da rede para suas instâncias do EC2. Quando a performance estiver fora da linha de base estabelecida, talvez seja necessário reconfigurar ou otimizar a instância para reduzir a utilização da CPU, melhorar a E/S de disco ou reduzir o tráfego de rede.

Para estabelecer uma linha de base, é preciso, no mínimo, monitorar os seguintes itens:

Item a ser monitorado	Métrica do Amazon EC2	Monitoramento do agente/ CloudWatch Logs
Utilização da CPU	CPUUtilization (p. 901)	
Utilização da rede	NetworkIn (p. 901) NetworkOut (p. 901)	
Performance do disco	DiskReadOps (p. 901) DiskWriteOps (p. 901)	
Leituras/gravações de disco	DiskReadBytes (p. 901) DiskWriteBytes (p. 901)	
Utilização de memória, utilização de troca de disco, utilização de espaço em disco, utilização de arquivo de páginas, coleção de logs		[Instâncias Linux e Windows Server] Colecionar métricas e logs das instâncias do Amazon EC2 e servidores locais com o agente do CloudWatch [Migração de agentes anteriores do CloudWatch Logs em

Item a ser monitorado	Métrica do Amazon EC2	Monitoramento do agente/ CloudWatch Logs
		instâncias do Windows Server] Migrar coleção de logs da instância Windows Server para o agente do CloudWatch

Monitoramento automático e manual

A AWS fornece várias ferramentas que você pode usar para monitorar o Amazon EC2. É possível configurar algumas dessas ferramentas para fazer o monitoramento em seu lugar, e, ao mesmo tempo, algumas das ferramentas exigem intervenção manual.

Ferramentas de monitoramento

- [Ferramentas de monitoramento automatizadas \(p. 865\)](#)
- [Ferramentas de monitoramento manual \(p. 866\)](#)

Ferramentas de monitoramento automatizadas

Use as seguintes ferramentas de monitoramento automatizadas para observar o Amazon EC2 e gerar relatórios quando algo estiver errado:

- System status checks (Verificações do status do sistema): monitore os sistemas da AWS necessários para usar a instância a fim de garantir que eles estejam funcionando corretamente. Essas verificações detectam problemas com sua instância que exigem a participação da AWS para corrigi-los. Quando ocorre uma falha em uma verificação de status do sistema, você pode optar por esperar a AWS corrigir o problema ou resolvê-lo por conta própria (por exemplo, interrompendo e reiniciando ou encerrando e substituindo uma instância). Exemplos de problemas que causam falha nas verificações de status do sistema incluem:
 - Perda de conectividade de rede
 - Perda de energia do sistema
 - Problemas de software no host físico
 - Problemas de hardware de host físico que afetam a acessibilidade de rede

Para obter mais informações, consulte [Verificações de status para as instâncias \(p. 867\)](#).

- Verificações do status da instância – monitore o software e a configuração de rede da instância individual. Essas verificações detectam problemas que exigem seu envolvimento para correção. Quando ocorre uma falha em uma verificação de status da instância, normalmente, você precisará resolver o problema por conta própria (por exemplo, reinicializando a instância ou fazendo modificações no sistema operacional). Exemplos de problemas que podem causar falha nas verificações de status da instância incluem:
 - Verificações de status de sistema com falha
 - Configuração incorreta do startup ou da rede
 - Memória exaurida
 - Sistema de arquivos corrompido
 - Kernel incompatível

Para obter mais informações, consulte [Verificações de status para as instâncias \(p. 867\)](#).

- Alarmes do Amazon CloudWatch – observe uma única métrica ao longo de um período que você especificar e realize uma ou mais ações com base no valor da métrica em relação a determinado limite

ao longo de vários períodos. A ação é uma notificação enviada para um tópico do Amazon Simple Notification Service (Amazon SNS) ou por uma política do Amazon EC2 Auto Scaling. Os alertas invocam ações apenas para alterações de estado mantidas. Os alarmes do CloudWatch não invocarão ações simplesmente porque estão em um estado específico. O estado deve ter sido alterado e mantido por um número específico de períodos. Para obter mais informações, consulte [Monitorar instâncias usando o CloudWatch \(p. 898\)](#).

- Amazon EventBridge: automatize os produtos da AWS e responde automaticamente a eventos do sistema. Os eventos dos produtos da AWS são entregues ao EventBridge em tempo quase real, e você pode especificar ações automáticas a serem executadas quando um evento corresponde a uma regra elaborada por você. Para obter mais informações, consulte [O que é o Amazon EventBridge?](#).
- Amazon CloudWatch Logs: monitore, armazene e acesse os arquivos de log de instâncias do Amazon EC2, do AWS CloudTrail ou de outras origens. Para obter mais informações, consulte o [Amazon CloudWatch Logs User Guide](#) (Manual do usuário do Amazon CloudWatch Logs).
- Agente do CloudWatch – cole logs e métricas no nível do sistema de hosts e convidados nas instâncias do EC2 e nos servidores no local. Para obter mais informações, consulte [Coletar métricas e logs de instâncias do Amazon EC2 e de servidores no local com o agente do CloudWatch](#) no Guia do usuário do Amazon CloudWatch.
- AWS Management Pack for Microsoft System Center Operations Manager: vincula instâncias do Amazon EC2 e sistemas operacionais Windows ou Linux executados nelas. O AWS Management Pack é uma extensão do Microsoft System Center Operations Manager. Ele usa um computador designado no datacenter (chamado de nó observador) e APIs da Amazon Web Services para descobrir e coletar remotamente informações sobre os recursos da AWS. Para obter mais informações, consulte o [AWS Management Pack for Microsoft System Center \(p. 1661\)](#).

Ferramentas de monitoramento manual

Outra parte importante do monitoramento do Amazon EC2 envolve o monitoramento manual desses itens que os scripts de monitoramento, verificações de status e alarmes do CloudWatch não abrangem. Os painéis do console do Amazon EC2 e do CloudWatch fornecem uma visão rápida do estado do ambiente do Amazon EC2.

- O painel do Amazon EC2 mostra:
 - Eventos de integridade e programados por região
 - Estado da instância
 - Verificações do status
 - Status do alarme
 - Detalhes da métrica da instância (no painel de navegação, escolha Instances (Instâncias), selecione uma instância e escolha a guia Monitoring (Monitoramento))
 - Detalhes da métrica de volume (no painel de navegação, escolha Volumes, selecione um volume e escolha a guia Monitoring (Monitoramento))
- O painel do Amazon CloudWatch mostra:
 - Alertas e status atual
 - Gráficos de alertas e recursos
 - Estado de integridade do serviço

Além disso, você pode usar o CloudWatch para fazer o seguinte:

- Colocar em gráfico dados de monitoramento do Amazon EC2 para solucionar problemas e descobrir tendências
- Pesquisar e procurar todas as métricas de recursos da AWS
- Criar e editar alarmes para ser notificado sobre problemas
- Consulte as visões gerais rápidas dos alarmes e recursos da AWS

Melhores práticas de monitoramento

Use as melhores práticas de monitoramento a seguir para ajudá-lo com suas tarefas de monitoramento do Amazon EC2.

- Faça o monitoramento de uma prioridade para gerenciar problemas pequenos antes que eles se tornem grandes.
- Crie e implemente um plano de monitoramento que colete dados de monitoramento de todas as partes da solução da AWS para facilitar a depuração de uma falha de vários pontos (caso ocorra). Seu plano de monitoramento deve tratar, pelo menos, as seguintes questões:
 - Quais são seus objetivos de monitoramento?
 - Quais recursos você vai monitorar?
 - Com que frequência você vai monitorar esses recursos?
 - Quais ferramentas de monitoramento você usará?
 - Quem realizará o monitoramento das tarefas?
 - Quem deve ser notificado quando algo der errado?
- Automatize tarefas de monitoramento o máximo possível.
- Verifique os arquivos de log em suas instâncias do EC2.

Monitorar o status das instâncias

Você pode monitorar o status de suas instâncias visualizando as verificações de status e os eventos programados para elas.

A verificação de status fornece as informações resultantes de verificações automáticas executadas pelo Amazon EC2. Essas verificações automáticas detectam se problemas específicos estão afetando as instâncias. As informações de verificação de status, em conjunto com os dados fornecidos pelo Amazon CloudWatch, oferecem visibilidade operacional detalhada sobre cada uma das instâncias.

Também é possível ver o status de eventos específicos programados para suas instâncias. O status de eventos fornece informações sobre as próximas atividades que estão programadas para suas instâncias, como reinicialização ou desativação. Ele também fornece os horários de início e término programados para cada evento.

Tópicos

- [Verificações de status para as instâncias \(p. 867\)](#)
- [Eventos programados para instâncias \(p. 874\)](#)

Verificações de status para as instâncias

Com o monitoramento de status de instâncias, por exemplo, é possível determinar rapidamente se o Amazon EC2 detectou problemas que possam impedir que as instâncias executem aplicações. O Amazon EC2 executa verificações automáticas em cada instância do EC2 em execução para identificar problemas de hardware e software. Você pode visualizar os resultados dessas verificações de status para identificar problemas específicos e detectáveis. O status do evento expande as informações que o Amazon EC2 já fornece sobre o estado de cada instância (como pending, running, stopping) e as métricas de utilização que o Amazon CloudWatch monitora (utilização de CPU, tráfego de rede e atividade de disco).

As verificações de status são realizadas a cada minuto e elas retornam o status de aprovação e reprovação. Se todas as verificações forem aprovadas, o status geral da instância será OK. Se uma ou mais verificações falharem, o status geral será impaired. As verificações de status são integradas ao Amazon EC2, portanto elas não podem ser desabilitadas ou excluídas.

Quando uma verificação de status falha, a métrica do CloudWatch correspondente para as verificações de status é incrementada. Para obter mais informações, consulte [Métricas de verificação de status \(p. 908\)](#). É possível usar essas métricas para criar alarmes do CloudWatch que são acionados com base no resultado das verificações de status. Por exemplo, você pode criar um alarme para avisá-lo se as verificações de status falharem em uma instância específica. Para obter mais informações, consulte [Criar e editar alarmes de verificação de status \(p. 872\)](#).

Você também pode criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2 e recupere automaticamente a instância se ela for danificada devido a um problema subjacente. Para obter mais informações, consulte [Recuperar a instância \(p. 480\)](#).

Tópicos

- [Tipos de verificações de status \(p. 868\)](#)
- [Visualizar verificações de status \(p. 869\)](#)
- [Relatar status da instância \(p. 871\)](#)
- [Criar e editar alarmes de verificação de status \(p. 872\)](#)

Tipos de verificações de status

Há dois tipos de verificações de status: verificações de status de sistema e verificações de status de instância.

Verificações de status de sistema

As verificações de status do sistema monitoram os sistemas da AWS nos quais a instância é executada. Essas verificações detectam problemas subjacentes na instância que exigem o envolvimento da AWS para a correção. Quando uma verificação de status do sistema falha, você pode esperar que a AWS corrija o problema ou pode corrigi-lo por conta própria. Para instâncias baseadas no Amazon EBS, é possível interrompê-las e iniciá-las por conta própria, o que, na maioria dos casos, faz com que a instância seja migrada para um novo host. Para instâncias do Linux com armazenamento de instância, você pode encerrar e substituir a instância. Para instâncias do Windows, o volume raiz deve ser um volume do Amazon EBS. O armazenamento de instâncias não é compatível com o volume raiz. Observe que os volumes de armazenamento de instâncias são efêmeros e todos os dados são perdidos quando a instância é interrompida.

A seguir, temos exemplos de problemas que podem causar falha nas verificações de status do sistema:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de software no host físico
- Problemas de hardware de host físico que afetam a acessibilidade de rede

Note

Se você executar uma reinicialização do sistema operacional em uma instância bare metal, a verificação de status do sistema poderá retornar temporariamente um status de falha. Quando a instância ficar disponível, a verificação de status do sistema deve retornar um status de aprovação.

Verificações de status de instâncias

Verificações do status da instância monitorem o software e a configuração de rede da instância individual. O Amazon EC2 verifica a integridade da instância enviando uma solicitação de protocolo de resolução de endereço (ARP) para a interface de rede (NIC). Essas verificações detectam problemas que exigem seu envolvimento para correção. Quando uma verificação de status de instância falha, geralmente você precisa

lidar com o problema por conta própria (por exemplo, reinicializando a instância ou fazendo alterações de configuração da instância).

A seguir, temos exemplos de problemas que podem causar falhas nas verificações de status da instância:

- Verificações de status de sistema com falha
- Configuração incorreta de redes ou startup
- Memória exaurida
- Sistema de arquivos corrompido
- Durante a reinicialização da instância ou enquanto uma instância com armazenamento de instâncias do Windows estiver sendo empacotada, uma verificação de status de instância relatará uma falha até que a instância se torne disponível novamente.

Note

Se você executar uma reinicialização do sistema operacional em uma instância bare metal, a verificação de status da instância poderá retornar temporariamente um status de falha. Quando a instância ficar disponível, a verificação de status dela deve retornar um status de aprovação.

Visualizar verificações de status

O Amazon EC2 fornece várias formas de visualizar e trabalhar com verificações de status.

Visualizar status usando o console

É possível visualizar verificações de status usando o AWS Management Console.

New console

Para visualizar as verificações de status (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na página Instances (Instâncias), a coluna Status check (Verificações de status) lista o status operacional de cada instância.
4. Para visualizar o status de uma instância específica, selecione a instância e escolha a guia Status Checks (Verificações de status).

The screenshot shows the AWS Management Console interface for viewing instance status checks. At the top, there is a table listing three instances with their names, instance IDs, states, types, and status check details. The first instance, i-0c0186a12aab3741d, is selected, and its details are shown below. The 'Status checks' tab is active in the navigation bar. The status check section displays a green icon indicating a passed check for 'System reachability'. A note at the bottom of this section states: 'If your instance is unreachable for more than 20 minutes, the Open support case button becomes available so that you can contact the Support Center.' There is also a link to the 'Support Center' and 'Discussion Forums'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Avail
<input checked="" type="checkbox"/> -	i-0c0186a12aab3741d	Running	t2.large	1/2 checks ...	No alarms	eu-w
<input type="checkbox"/> -	i-0138edcaf722db475	Running	m4.large	2/2 checks ...	No alarms	eu-w
<input type="checkbox"/> -	i-02c65b735153975ec	Running	t3.medium	2/2 checks ...	No alarms	eu-w

Instance: i-0c0186a12aab3741d

Status checks Info
Status checks detect problems that may impair i-0c0186a12aab3741d from running your applications.

System status checks
System reachability check passed

Need assistance?
If your instance is unreachable for more than 20 minutes, the **Open support case** button becomes available so that you can contact the Support Center.

Open support case

Visit the [Support Center](#) or post a question to the [Discussion Forums](#)

Instance status checks
Instance reachability check failed
Check failure at
2020/12/16 17:30 GMT+2 (about 1 month)

Se a verificação de status da instância falhar, você normalmente precisará lidar com o problema por conta própria (por exemplo, reinicializando a instância ou fazendo alterações de configuração da instância). Porém, se a instância falhar na verificação de status e ela permanecer inacessível por mais de 20 minutos, escolha Open support case (Abrir caso de suporte) para enviar uma solicitação de assistência.

5. Para revisar as métricas do CloudWatch para verificações de status, selecione a instância e a guia Monitoring (Monitoramento). Role até ver os gráficos das seguintes métricas:
 - Status check failed (any) (Falha na verificação de status (qualquer))
 - Status check failed (instance) (Falha na verificação de status (instância))
 - Status check failed (system) (Falha na verificação de status (sistema))

Old console

Para visualizar as verificações de status (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na página Instances, a coluna Status Checks lista o status operacional de cada instância.
4. Para visualizar o status de uma instância específica, selecione a instância e escolha a guia Status Checks.

The screenshot shows the 'Status Checks' tab selected in the AWS EC2 Instances page. It displays two sections: 'System Status Checks' and 'Instance Status Checks'. The 'System Status Checks' section shows a green status bar with the message 'System reachability check passed'. The 'Instance Status Checks' section shows a red status bar with the message 'Instance reachability check failed at October 7, 2013 11:52:11 AM UTC+2 (16 minutes ago)'. Below these sections, there is a note: 'These checks monitor your software and network configuration for this instance. Learn more about this issue.'

Se houver uma instância falhar na verificação de status, e ela estiver inacessível por mais de 20 minutos, escolha AWS Support para enviar uma solicitação de assistência.

5. Para revisar as métricas do CloudWatch para verificações de status, selecione a instância e a guia Monitoring (Monitoramento). Role até ver os gráficos das seguintes métricas:
 - Status Check Failed (Any) (Falha na verificação de status (qualquer))
 - Status Check Failed (Instance) (Falha na verificação de status (instância))
 - Status Check Failed (System) (Falha na verificação de status (sistema))

Visualizar status usando a linha de comando

É possível visualizar as verificações de status de instâncias em execução usando o comando `describe-instance-status` (AWS CLI).

Para visualizar o status de todas as instâncias, use o comando a seguir.

```
aws ec2 describe-instance-status
```

Para obter o status de todas as instâncias com um status de `impaired`, use o comando a seguir.

```
aws ec2 describe-instance-status \
```

```
--filters Name=instance-status.status,Values=impaired
```

Para obter o status de uma única instância, use o comando a seguir.

```
aws ec2 describe-instance-status \
--instance-ids i-1234567890abcdef0
```

Como alternativa, use os seguintes comandos do :

- [Get-EC2InstanceState](#) (AWS Tools for Windows PowerShell)
- [DescribeInstanceStatus](#) (API de consulta do Amazon EC2)

Relatar status da instância

É possível fornecer feedback se você estiver tendo problemas com uma instância cujo status não é mostrado como danificado ou se você quiser enviar detalhes adicionais à AWS sobre os problemas que está enfrentando com uma instância danificada.

Usamos o feedback enviado para identificar problemas que impactam vários clientes, mas não respondemos a problemas de conta individuais. O fornecimento de feedback não altera os resultados da verificação de status que você vê atualmente para a instância.

Relatar feedback do status usando o console

New console

Para relatar o status de instâncias (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha a guia Status Checks (Verificações de status), escolha Actions (Ações) (o segundo menu Actions (Ações) na metade inferior da página) e selecione Report instance status (Relatar status da instância).
4. Preencha o formulário Report instance status (Relatar status da instância) e escolha Submit (Enviar).

Old console

Para relatar o status de instâncias (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha a guia Status Checks (Verificações de status) e escolha Submit feedback (Enviar comentários).
4. Preencha o formulário Report Instance Status e escolha Submit.

Relatar feedback do status usando a linha de comando

Use o comando [report-instance-status](#) (AWS CLI) para enviar feedback sobre o status de uma instância danificada.

```
aws ec2 report-instance-status \
```

```
--instances i-1234567890abcdef0 \
--status impaired \
--reason-codes code
```

Como alternativa, use os seguintes comandos :

- [Send-EC2InstanceState](#) (AWS Tools for Windows PowerShell)
- [ReportInstanceState](#) (API de consulta do Amazon EC2)

Criar e editar alarmes de verificação de status

É possível usar as [métricas de verificação de status \(p. 908\)](#) para criar alarmes do CloudWatch a fim de notificar você quando uma instância apresentou falha na verificação de status.

Criar um alarme de verificação de status usando o console

Use o procedimento a seguir para configurar um alarme que envia uma notificação por e-mail ou que interrompe, encerra ou recupera uma instância quando ela apresenta falha em uma verificação de status.

New console

Para criar um alarme de verificação de status (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha a guia Status Checks (Verificações de status) e selecione Actions (Ações), Create status check alarm (Criar alarme de verificação de status).
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), em Add or edit alarm (Adicionar ou editar alarme), selecione Create an alarm (Criar um alarme).
5. Em Alarm notification (Notificação de alarme), ative a opção para configurar notificações do Amazon Simple Notification Service (Amazon SNS). Selecione um tópico existente do Amazon SNS ou insira um nome para criar um tópico.

Se você tiver adicionado um endereço de e-mail à lista de destinatários ou criado um novo tópico, o Amazon SNS enviará uma mensagem de e-mail de confirmação de assinatura para cada novo endereço. Cada destinatário deve confirmar a assinatura escolhendo o link contido na mensagem. As notificações de alerta são enviadas apenas para endereços confirmados.

6. Em Alarm action (Ação de alarme), ative a opção para especificar uma ação a ser executada quando o alarme for acionado. Selecione a ação.
7. Em Alarm thresholds (Limites de alarme), especifique a métrica e os critérios do alarme.

Você pode deixar as configurações padrão para Group samples by (Average) (Agrupar amostras por (Média)) e Type of data to sample (Status check failed: either) (Tipo de dados para amostragem (Falha na verificação de status: qualquer)) ou pode alterá-los para atender às suas necessidades.

Para Consecutive Period (Período consecutivo), defina o número de períodos que deseja avaliar e, em Period (Período), insira a duração do período de avaliação antes de acionar o alarme e enviar um e-mail.

8. (Opcional) Em Sample metric data (Dados de métrica de exemplo), escolha Add to dashboard (Adicionar ao painel).
9. Escolha Create (Criar).

Old console

Para criar um alarme de verificação de status (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha a guia Status Checks (Verificações de status) e escolha Create Status Check Alarm (Criar alarme da verificação de status).
4. Selecione Send a notification to. Escolha um tópico SNS existente ou escolha create topic (criar tópico) para criar um novo. Se criar um novo tópico, em With these recipients, insira seu endereço de e-mail e os endereços de destinatários adicionais, separados por vírgulas.
5. (Opcional) Selecione Take the action (Executar a ação) e selecione a ação que gostaria de executar.
6. Em Whenever, selecione a verificação de status da qual deseja ser notificado.

Se você tiver selecionado Recover this instance na etapa anterior, selecione Status Check Failed (System).
7. Em For at least, defina o número de períodos que deseja avaliar, e em consecutive periods, selecione a duração do período de avaliação antes de disparar o alarme e enviar um e-mail.
8. (Opcional) Em Name of alarm, substitua o nome padrão por outro nome para o alarme.
9. Escolha Create Alarm.

Important

Se você tiver adicionado um endereço de e-mail à lista de destinatários ou criado um novo tópico, o Amazon SNS enviará uma mensagem de e-mail de confirmação de assinatura para cada novo endereço. Cada destinatário deve confirmar a assinatura escolhendo o link contido na mensagem. As notificações de alerta são enviadas apenas para endereços confirmados.

Se você precisar fazer alterações em um alarme de status de instância, poderá editá-lo.

New console

Como editar um alarme de verificação de status usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitoring (Monitoramento), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).
4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), em Add or edit alarm (Adicionar ou editar alarme), escolha Edit an alarm (Editar um alarme).
5. Em Search for alarm (Procurar alarme), escolha o alarme.
6. Quando terminar de fazer alterações, escolha Update (Atualizar).

Old console

Como editar um alarme de verificação de status usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), CloudWatch Monitoring (Monitoramento do CloudWatch) e escolha Add/Edit Alarms (Adicionar/editar alarmes).
4. Na caixa de diálogo Alarm Details, escolha o nome do alarme.

5. Na caixa de diálogo Edit Alarm, faça as alterações desejadas e escolha Save.

Criar um alarme de verificação de status usando a AWS CLI

No exemplo a seguir, o alarme publica uma notificação para um tópico de SNS, `arn:aws:sns:us-west-2:111122223333:my-sns-topic`, quando há falha da instância na verificação de instância ou na verificação de status de sistema por, pelo menos, dois períodos consecutivos. A métrica do CloudWatch usada é `StatusCheckFailed`.

Como criar um alarme de verificação de status usando a AWS CLI

1. Selecione um tópico de SNS existente ou crie um novo. Para obter mais informações, consulte [Using the AWS CLI with Amazon SNS](#) (Usar a AWS CLI com a VPC), no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).
2. Use o seguinte comando `list-metrics` para visualizar as métricas do Amazon CloudWatch disponíveis para o Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Use o seguinte comando `put-metric-alarm` para criar o alarme.

```
aws cloudwatch put-metric-alarm --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 --metric-name StatusCheckFailed --namespace AWS/EC2 --statistic Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 --unit Count --period 300 --evaluation-periods 2 --threshold 1 --comparison-operator GreaterThanOrEqualToThreshold --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

O período é o intervalo de tempo, em segundos, no qual as métricas do Amazon CloudWatch são coletadas. Este exemplo usa 300, que são 60 segundos multiplicados por 5 minutos. O período de avaliação é o número de períodos consecutivos pelos quais o valor da métrica deve ser comparado ao limite. Este exemplo usa 2. As ações do alarme são as ações a serem executadas quando esse alarme é acionado. Este exemplo configura o alarme para enviar um e-mail usando Amazon SNS.

Eventos programados para instâncias

AWS pode programar eventos para suas instâncias, como reinicialização, interrupção/início ou retirada. Esses eventos não ocorrem com frequência. Se uma de suas instâncias for afetada por um evento programado, a AWS enviará um e-mail ao endereço de e-mail que estiver associado à sua conta da AWS antes do evento programado. O e-mail fornece detalhes sobre o evento, incluindo as datas de início e de término. Dependendo do evento, você pode tomar providências para controlar sua duração. A AWS também envia um evento do AWS Health, que é possível monitorar e gerenciar usando o Amazon CloudWatch Events. Para obter mais informações sobre o monitoramento de eventos do AWS Health com CloudWatch, consulte [Monitoring AWS Health events with CloudWatch Events](#) (Monitorar eventos do AWS Health com CloudWatch Events).

Os eventos programados são gerenciados pela AWS. Você não pode programar eventos para suas instâncias. Você pode exibir os eventos programados pela AWS, personalizar notificações de eventos programados para incluir ou remover tags da notificação por e-mail, executar ações quando uma instância estiver programada para ser reinicializada, desativada ou interrompida.

Para atualizar as informações de contato de sua conta a fim de ter certeza de que será notificado sobre os eventos agendados, acesse a página [Configurações da conta](#).

Tópicos

- [Tipos de eventos programados \(p. 875\)](#)

- [Visualizar eventos agendados \(p. 875\)](#)
- [Personalizar notificações de eventos programados \(p. 879\)](#)
- [Trabalhar com instâncias programadas para interrupção ou retirada \(p. 881\)](#)
- [Trabalhar com instâncias programadas para reinicialização \(p. 882\)](#)
- [Trabalhar com instâncias programadas para manutenção \(p. 883\)](#)
- [Reagendar um evento programado \(p. 884\)](#)
- [Definir janelas de eventos para eventos programados \(p. 886\)](#)

Tipos de eventos programados

O Amazon EC2 pode criar os seguintes tipos de eventos para suas instâncias, onde o evento ocorre em um horário programado:

- Instance stop (Interrupção de instância): na hora programada, a instância é interrompida. Quando você iniciá-la novamente, ela será migrada para um novo host. Aplica-se somente a instâncias baseadas no Amazon EBS.
- Instance retirement (Desativação da instância): na hora programada a instância é interrompida, se for baseada no Amazon EBS, ou encerrada, se for baseada no armazenamento de instâncias.
- Instance reboot (Reinicialização de instância): na hora programada, a instância é reinicializada.
- System reboot (Reinicialização do sistema): na hora programada, o host da instância é reinicializado.
- System maintenance (Manutenção do sistema): na hora programada, a instância pode ser temporariamente afetada pela manutenção de rede ou pela manutenção de energia.

Visualizar eventos agendados

Além de receber a notificação de eventos agendados por e-mail, você pode verificar se há eventos programados usando um dos métodos a seguir.

New console

Para visualizar os eventos programados para suas instâncias usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Você pode exibir eventos agendados nas seguintes telas:
 - No painel de navegação, selecione Events. Todos os recursos com um evento associado serão exibidos. É possível filtrar por Resource ID (ID do recurso), Resource type (Tipo de recurso), Availability zone (Zona de disponibilidade), Event status (Status do evento) ou Event type (Tipo de evento).

Events (103)						
Actions						
Resource type: instance		Event status: Scheduled		Event type: instance-stop		Clear filters
Resource ID	Event status	Event type	Description	Progress	Duration	Start time
i-02c48ffba61cd16f	Scheduled	instance-stop	The instance is running on ...	Starts in 13 days		2019/07/22 13:00 GMT+2

- Como opção, no painel de navegação, escolha EC2 Dashboard. Todos os recursos com um evento associado serão exibidos em Eventos agendados.

Scheduled events	C
US East (N. Virginia)	
• 7 instance(s) have scheduled events	
• 1 volume(s) are impaired	

Old console

Para visualizar os eventos programados para suas instâncias usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Você pode exibir eventos agendados nas seguintes telas:
 - No painel de navegação, selecione Events. Todos os recursos com um evento associado serão exibidos. Você pode filtrar por tipo de recurso ou por tipos de eventos específicos. É possível selecionar o recurso para visualizar detalhes.

The screenshot shows the AWS EC2 Events interface. At the top, there are three dropdown filters: 'All resource types' (selected), 'All event types' (selected), and 'Ongoing and scheduled' (selected). Below the filters is a search bar with a dropdown menu for 'Resource Name'. The search results table has columns for 'Resource Name', 'Resource Type', 'Resource Id', and 'Event Type'. One result is listed: 'my-instance' under 'Resource Name', 'instance' under 'Resource Type', 'i-c3870335' under 'Resource Id', and 'instance-stop' under 'Event Type'.

Event: i-c3870335

Availability Zone	us-west-2a
Event type	instance-stop
Event status	Scheduled
Description	The instance is running on degraded hardware
Start time	May 22, 2015 at 5:00:00 PM UTC-7
End time	

- Como opção, no painel de navegação, escolha EC2 Dashboard. Todos os recursos com um evento associado serão exibidos em Scheduled Events.

Scheduled Events

US West (Oregon):

1 instances have scheduled events

- Alguns eventos também são mostrados para recursos afetados. Por exemplo, no painel de navegação, escolha Instances (Instâncias) e selecione uma instância. Se a instância tiver um evento de desativação ou interrupção de instância associado, ele será exibido no painel inferior.



Retiring: This instance is scheduled for retirement after May 22, 2015 at 5:00:00 PM UTC-7. (i)

AWS CLI

Para visualizar os eventos programados para suas instâncias usando a AWS CLI

Use o comando `describe-instance-status`.

```
aws ec2 describe-instance-status \
--instance-id i-1234567890abcdef0 \
--query "InstanceStatuses[ ].Events"
```

O exemplo de saída a seguir mostra um evento de reinicialização.

```
[  
    "Events": [  
        {  
            "InstanceEventId": "instance-event-0d59937288b749b32",  
            "Code": "system-reboot",  
            "Description": "The instance is scheduled for a reboot",  
            "NotAfter": "2019-03-15T22:00:00.000Z",  
            "NotBefore": "2019-03-14T20:00:00.000Z",  
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"  
        }  
    ]  
]
```

O exemplo de saída a seguir mostra um evento de desativação de instância:

```
[  
    "Events": [  
        {  
            "InstanceEventId": "instance-event-0e439355b779n26",  
            "Code": "instance-stop",  
            "Description": "The instance is running on degraded hardware",  
            "NotBefore": "2015-05-23T00:00:00.000Z"  
        }  
    ]  
]
```

PowerShell

Para visualizar os eventos programados para suas instâncias usando a AWS Tools for Windows PowerShell

Use o seguinte comando [Get-EC2InstanceState](#).

```
PS C:\> (Get-EC2InstanceState -InstanceId i-1234567890abcdef0).Events
```

O exemplo de saída a seguir mostra um evento de desativação de instância:

```
Code      : instance-stop  
Description : The instance is running on degraded hardware  
NotBefore : 5/23/2015 12:00:00 AM
```

Instance metadata

Para visualizar os eventos programados para suas instâncias usando metadados de instância

É possível recuperar informações sobre eventos de manutenção ativos para suas instâncias dos [metadados de instância \(p. 622\)](#) usando o Serviço de metadados da instância versão 2 ou o Serviço de metadados da instância versão 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/scheduled
```

A seguir, temos um exemplo de saída com informações sobre um evento de reinicialização do sistema programado, no formato JSON.

```
[  
 {  
     "NotBefore" : "21 Jan 2019 09:00:43 GMT",  
     "Code" : "system-reboot",  
     "Description" : "scheduled reboot",  
     "EventId" : "instance-event-0d59937288b749b32",  
     "NotAfter" : "21 Jan 2019 09:17:23 GMT",  
     "State" : "active"  
 }  
]
```

Para visualizar o histórico de eventos sobre eventos concluídos ou cancelados das suas instâncias usando metadados de instância

É possível recuperar informações sobre eventos concluídos ou cancelados para suas instâncias dos [metadados de instância \(p. 622\)](#) usando o Serviço de metadados da instância versão 2 ou o Serviço de metadados da instância versão 1.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-  
ec2-metadata-token-ttl-seconds: 21600"` \  
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-  
data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

A seguir, temos um exemplo de saída com informações sobre um evento de reinicialização do sistema que foi cancelado e um que foi concluído, no formato JSON.

```
[  
 {  
     "NotBefore" : "21 Jan 2019 09:00:43 GMT",  
     "Code" : "system-reboot",  
     "Description" : "[Canceled] scheduled reboot",  
     "EventId" : "instance-event-0d59937288b749b32",  
     "NotAfter" : "21 Jan 2019 09:17:23 GMT",  
     "State" : "canceled"  
 },  
 {  
     "NotBefore" : "29 Jan 2019 09:00:43 GMT",  
     "Code" : "system-reboot",  
     "Description" : "[Completed] scheduled reboot",  
     "EventId" : "instance-event-0d59937288b749b32",  
     "NotAfter" : "29 Jan 2019 09:17:23 GMT",  
     "State" : "completed"  
 }  
]
```

AWS Health

Você pode usar o AWS Personal Health Dashboard para saber mais sobre eventos que podem afetar a instância. O AWS Personal Health Dashboard organiza problemas em três grupos: ocorrências

abertas, alterações programadas e outras notificações. O grupo de alterações programadas contém itens presentes e futuros.

Para obter mais informações, consulte [Getting started with the AWS Personal Health Dashboard](#) (Conceitos básicos do AWS Personal Health Dashboard) no AWS Health User Guide (Manual do usuário do AWS Health).

Personalizar notificações de eventos programados

É possível personalizar notificações de eventos programados para incluir tags na notificação por e-mail. Isso facilita a identificação do recurso afetado (instâncias ou Hosts dedicados) e priorizar ações para o próximo evento.

Ao personalizar notificações de eventos para incluir tags, você pode optar por incluir:

- Todas as tags associadas ao recurso afetado
- Somente tags específicas que estão associadas ao recurso afetado

Por exemplo, suponha que você atribua as tags `application`, `costcenter`, `project` e `owner` a todas as suas instâncias. É possível optar por incluir todas as tags nas notificações de eventos. Como alternativa, se você quiser ver apenas as tags `owner` e `project` nas notificações de eventos, poderá optar por incluir apenas essas tags.

Depois de selecionar as tags a serem incluídas, as notificações de evento incluirão o ID do recurso (ID da instância ou ID do Host dedicado) e os pares de chave de tag e valor associados ao recurso afetado.

Tópicos

- [Incluir tags em notificações de eventos \(p. 879\)](#)
- [Remover tags de notificações de eventos \(p. 880\)](#)
- [Visualizar as tags a serem incluídas nas notificações de eventos \(p. 881\)](#)

Incluir tags em notificações de eventos

As tags que você escolher incluir se aplicarão a todos os recursos (instâncias e Hosts dedicados) na região selecionada. Para personalizar notificações de eventos em outras regiões, primeiro selecione a região necessária e execute as etapas a seguir.

É possível incluir tags em notificações de eventos usando um dos métodos a seguir.

New console

Como incluir tags em notificações de eventos

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Escolha Actions (Ações), Manage event notifications (Gerenciar notificações de eventos).
4. Selecione **Include resource tags in event notifications** (Incluir tags de recurso em notificações de eventos).
5. Siga um destes procedimentos, dependendo das tags que você deseja incluir nas notificações de eventos:
 - Para incluir todas as tags associadas à instância afetada ou ao Host dedicado, selecione **Include all resource tags** (Incluir todas as tags de recurso).

- Para selecionar manualmente as tags a serem incluídas, selecione Choose the tags to include (Escolher as tags a serem incluídas) e em Choose the tags to include (Escolher as tags a serem incluídas), insira a chave de tag e pressione Enter.
6. Escolha Save (Salvar).

AWS CLI

Como incluir todas as tags em notificações de eventos

Use o comando [register-instance-event-notification-attributes](#) da AWS CLI e defina o parâmetro `IncludeAllTagsOfInstance` como `true`.

```
aws ec2 register-instance-event-notification-attributes --instance-tag-attribute  
"IncludeAllTagsOfInstance=true"
```

Como incluir tags específicas em notificações de eventos

Use o comando [register-instance-event-notification-attributes](#) da AWS CLI e especifique as tags a serem incluídas usando o parâmetro `InstanceTagKeys`.

```
aws ec2 register-instance-event-notification-attributes --instance-tag-attribute  
'InstanceTagKeys=[ "tag_key_1", "tag_key_2", "tag_key_3" ]'
```

Remover tags de notificações de eventos

É possível remover tags de notificações de eventos usando um dos métodos a seguir.

New console

Como remover tags de notificações de eventos

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Escolha Actions (Ações), Manage event notifications (Gerenciar notificações de eventos).
4. Siga um destes procedimentos, dependendo da tag a ser removida das notificações de eventos.
 - Para remover todas as tags das notificações de eventos, desmarque `Include resource tags in event notifications` (Incluir tags de recurso nas notificações de eventos).
 - Para remover tags específicas das notificações de eventos, escolha Remove (Remover) (X) para as tags listadas abaixo do campo `Choose the tags to include` (Escolher as tags a serem incluídas).
5. Escolha Save (Salvar).

AWS CLI

Como remover todas as tags das notificações de eventos

Use o comando [deregister-instance-event-notification-attributes](#) da AWS CLI e defina o parâmetro `IncludeAllTagsOfInstance` como `false`.

```
aws ec2 deregister-instance-event-notification-attributes --instance-tag-attribute  
"IncludeAllTagsOfInstance=false"
```

Como remover tags específicas de notificações de eventos

Use o comando [deregister-instance-event-notification-attributes](#) da AWS CLI e especifique as tags a serem removidas usando o parâmetro `InstanceTagKeys`.

```
aws ec2 deregister-instance-event-notification-attributes --instance-tag-attribute  
'InstanceTagKeys=[ "tag_key_1", "tag_key_2", "tag_key_3" ]'
```

Visualizar as tags a serem incluídas nas notificações de eventos

É possível visualizar as tags que devem ser incluídas nas notificações de eventos usando um dos métodos a seguir.

New console

Como visualizar as tags a serem incluídas nas notificações de eventos

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Escolha Actions (Ações), Manage event notifications (Gerenciar notificações de eventos).

AWS CLI

Como visualizar as tags a serem incluídas nas notificações de eventos

Use o comando [describe-instance-event-notification-attributes](#) da AWS CLI.

```
aws ec2 describe-instance-event-notification-attributes
```

Trabalhar com instâncias programadas para interrupção ou retirada

Quando a AWS detecta falha irreparável do host subjacente para sua instância, ela programa a instância para ser interrompida ou encerrada, dependendo do tipo de dispositivo raiz da instância. Se o dispositivo raiz for um volume do EBS, a instância será programada para ser interrompida. Se o dispositivo raiz for um volume de armazenamento de instância, a instância será programada para encerrar. Para obter mais informações, consulte [Desativação da instância \(p. 471\)](#).

Important

Todos os dados armazenados nos volumes de armazenamento de instâncias serão perdidos quando a instância for interrompida, hibernada ou encerrada. Isso inclui volumes de armazenamento de instância anexados a uma instância que possui um volume do EBS como dispositivo raiz. Lembre-se de salvar os dados dos volumes do armazenamento de instâncias que poderão ser necessários mais tarde antes que a instância seja interrompida, hibernada ou encerrada.

Ações para instâncias baseadas no Amazon EBS

Você pode esperar que a instância seja interrompida conforme programado. Como opção, você pode interromper e iniciar a instância por conta própria, o que a fará migrar para um novo host. Para obter mais informações sobre como interromper a instância, além de informações sobre as mudanças em sua configuração de instância quando ela estiver interrompida, consulte [Interromper e iniciar sua instância \(p. 455\)](#).

É possível automatizar uma interrupção e inicialização imediatas em resposta a um evento programado de interrupção de instância. Para obter mais informações, consulte [Automating Actions for EC2 Instances](#)

(Automatizar ações para instâncias do EC2) no AWS Health User Guide (Manual do usuário do AWS Health).

Ações para instâncias com armazenamento de instâncias

Recomendamos que você execute uma instância de substituição da AMI mais recente e migre todos os dados necessários para a instância de substituição antes que a instância seja programada para encerrar. Depois, você pode encerrar a instância original ou esperar que ela seja encerrada conforme programado.

Trabalhar com instâncias programadas para reinicialização

Quando a AWS precisa realizar tarefas, como instalar atualizações ou manter o host subjacente, ela pode programar a reinicialização da instância ou do host subjacente. É possível [reprogramar a maioria dos eventos de reinicialização \(p. 884\)](#) para que a instância seja reinicializada em uma data e hora específicas que sejam adequadas para você.

Se você interromper sua [instância do EC2 \(p. 1110\)](#) vinculada, ela será automaticamente desvinculada da VPC e os grupos de segurança da VPC não estarão mais associados à instância. Você pode vincular sua instância à VPC novamente depois de reiniciá-la.

Visualizar o tipo de evento de reinicialização

É possível ver se um evento de reinicialização é uma reinicialização de instância ou uma reinicialização do sistema usando um dos métodos a seguir.

New console

Para visualizar o tipo de evento de reinicialização programado usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Escolha Resource type: instance (Tipo de recurso: instância) na lista de filtros.
4. Para cada instância, visualize o valor na coluna Event type (Tipo de evento). O valor é system-reboot ou instance-reboot.

Old console

Para visualizar o tipo de evento de reinicialização programado usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Selecione Instance resources (Recursos da instância) na lista de filtros.
4. Para cada instância, visualize o valor na coluna Event type (Tipo de evento). O valor é system-reboot ou instance-reboot.

AWS CLI

Para visualizar o tipo de evento de reinicialização programado usando a AWS CLI

Use o comando [describe-instance-status](#).

```
aws ec2 describe-instance-status --instance-id i-1234567890abcdef0
```

Para eventos de reinicialização programados, o valor de Code é system-reboot ou instance-reboot. O seguinte exemplo de saída mostra um evento system-reboot.

```
[  
  "Events": [  
    {  
      "InstanceEventId": "instance-event-0d59937288b749b32",  
      "Code": "system-reboot",  
      "Description": "The instance is scheduled for a reboot",  
      "NotAfter": "2019-03-14T22:00:00.000Z",  
      "NotBefore": "2019-03-14T20:00:00.000Z",  
      "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"  
    }  
  ]  
]
```

Ações para reinicialização de instância

Você pode aguardar para que a reinicialização da instância ocorra dentro de sua janela de manutenção programada, [reprogramar \(p. 884\)](#) a reinicialização da instância para uma data e hora que sejam adequadas para você ou [reiniciar \(p. 470\)](#) a instância por conta própria em um momento conveniente.

Após a reinicialização da instância, o evento programado será apagado e a descrição dele será atualizada. A manutenção pendente do host subjacente será concluída e você poderá começar a usar a instância novamente depois que ela tiver sido totalmente reinicializada.

Ações para a reinicialização do sistema

Você não pode reiniciar o sistema por conta própria. Você pode aguardar para que a reinicialização do sistema ocorra durante a janela de manutenção programada, ou pode [reprogramar \(p. 884\)](#) a reinicialização do sistema para uma data e hora que sejam adequadas para você. Normalmente, uma reinicialização de sistema é concluída em questão de minutos. Depois que a reinicialização do sistema ocorre, a instância mantém o endereço IP e o nome de DNS, e qualquer dado nos volumes de armazenamento de instâncias locais é preservado. Depois que a reinicialização do sistema é concluída, o evento programado para a instância é apagado, e você pode verificar se o software da instância está operando conforme o esperado.

Como opção, se for necessário manter a instância em um horário diferente e você não puder reprogramar a reinicialização do sistema, não será possível interromper e iniciar a instância baseada em Amazon EBS, de modo que ela será migrada para um novo host. No entanto, os dados dos volumes de armazenamento de instâncias locais não são preservados. Também é possível automatizar uma interrupção e inicialização imediatas da instância em resposta a um evento programado de inicialização do sistema. Para obter mais informações, consulte [Automating Actions for EC2 Instances](#) (Automatizar ações para instâncias do EC2) no AWS Health User Guide (Manual do usuário do AWS Health). Para uma instância baseada no armazenamento de instâncias, se não for possível reprogramar a reinicialização do sistema, você poderá executar uma instância de substituição da AMI mais recente, migrar todos os dados necessários para a instância de substituição antes da janela de manutenção programada e encerrar a instância original.

Trabalhar com instâncias programadas para manutenção

Quando a AWS precisa manter o host subjacente de uma instância, ela programa a instância para manutenção. Há dois tipos de eventos de manutenção: manutenção de rede e manutenção de energia.

Durante a manutenção de rede, instâncias programadas perdem a conectividade de rede durante um breve período. A conectividade de rede normal com a instância é restaurada depois que a manutenção for concluída.

Durante a manutenção de energia, as instâncias programadas ficam offline durante um breve período e depois são reinicializadas. Quando uma reinicialização é realizada, todas as definições de configuração da instância são mantidas.

Depois que sua instância tiver sido reinicializada (isso geralmente leva alguns minutos), verifique se a aplicação está funcionando conforme o esperado. Nesse ponto, a instância não deve mais ter um evento associado a ela ou, se tiver, a descrição do evento programado começará com [Completed]. Às vezes, leva até 1 hora para que a descrição do status da instância seja atualizada. Eventos de manutenção concluídos são exibidos no painel do console do Amazon EC2 por até uma semana.

Ações para instâncias baseadas no Amazon EBS

Você pode esperar que a manutenção ocorra conforme programado. Como opção, você pode interromper e iniciar a instância, o que a fará migrar para um novo host. Para obter mais informações sobre como interromper a instância, além de informações sobre as mudanças em sua configuração de instância quando ela estiver interrompida, consulte [Interromper e iniciar sua instância \(p. 455\)](#).

É possível automatizar uma interrupção e inicialização imediatas em resposta a um evento programado de manutenção. Para obter mais informações, consulte [Automating Actions for EC2 Instances](#) (Automatizar ações para instâncias do EC2) no AWS Health User Guide (Manual do usuário do AWS Health).

Ações para instâncias com armazenamento de instâncias

Você pode esperar que a manutenção ocorra conforme programado. Como alternativa, se quiser manter a operação normal durante a janela de manutenção programada, você pode iniciar uma instância de substituição da AMI mais recente, migrar todos os dados necessários para a instância de substituição antes da janela de manutenção programada e, então, encerrar a instância original.

Reagendar um evento programado

É possível reagendar um evento para que ele ocorra em uma data e hora específicas que forem convenientes. Somente eventos que tenham uma data de prazo podem ser reprogramados. Há outras [limitações para reprogramar um evento \(p. 885\)](#).

É possível reagendar um evento usando um dos métodos a seguir.

New console

Como reprogramar um evento usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Escolha Resource type: instance (Tipo de recurso: instância) na lista de filtros.
4. Escolha uma ou mais instâncias e selecione Actions (Ações), Schedule event (Programar evento).

Somente eventos que têm uma data de prazo de evento, indicados por um valor para Deadline (Prazo), podem ser reprogramados. Se um dos eventos selecionados não tiver uma data de prazo, a opção Actions (Ações), Schedule event (Programar evento) será desativada.

5. Em New start time (Nova hora de início), insira uma nova data e hora para o evento. A nova data e hora devem ocorrer antes de Event deadline (Prazo do evento).
6. Escolha Save (Salvar).

Pode levar de um a dois minutos para a hora de início do evento atualizado ser refletida no console.

Old console

Como reprogramar um evento usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, selecione Events.
3. Selecione Instance resources (Recursos da instância) na lista de filtros.
4. Escolha uma ou mais instâncias e selecione Actions (Ações), Schedule Event (Programar evento).

Somente eventos que têm uma data de prazo de evento, indicados por um valor para Event Deadline (Prazo do evento), podem ser reprogramados.

5. Para Event start time (Hora de início do evento), insira uma nova data e hora para o evento. A nova data e hora devem ocorrer antes de Event Deadline (Prazo do evento).
6. Selecione Schedule Event (Programar evento).

Pode levar de um a dois minutos para a hora de início do evento atualizado ser refletida no console.

AWS CLI

Como reprogramar um evento usando a AWS CLI

1. Somente eventos que têm uma data de prazo de evento, indicados por um valor para NotBeforeDeadline, podem ser reprogramados. Use o comando [describe-instance-status](#) para visualizar o valor do parâmetro NotBeforeDeadline.

```
aws ec2 describe-instance-status --instance-id i-1234567890abcdef0
```

O seguinte exemplo de saída mostra um evento system-reboot que pode ser reprogramado, pois NotBeforeDeadline contém um valor.

```
[{"Events": [{"InstanceEventId": "instance-event-0d59937288b749b32", "Code": "system-reboot", "Description": "The instance is scheduled for a reboot", "NotAfter": "2019-03-14T22:00:00.000Z", "NotBefore": "2019-03-14T20:00:00.000Z", "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"}]}
```

2. Para reprogramar o evento, use o comando [modify-instance-event-start-time](#). Especifique a nova hora de início do evento usando o parâmetro not-before. A nova hora do evento deve ser antes de NotBeforeDeadline.

```
aws ec2 modify-instance-event-start-time --instance-id i-1234567890abcdef0 --instance-event-id instance-event-0d59937288b749b32 --not-before 2019-03-25T10:00:00.000
```

O comando [describe-instance-status](#) poderá levar de um a dois minutos para retornar o valor do parâmetro not-before atualizado.

Limitations

- Somente eventos com uma data de prazo podem ser reprogramados. O evento pode ser reprogramado até a data de prazo do evento. A coluna Deadline (Prazo) do console e o campo NotBeforeDeadline da AWS CLI indicam se o evento tem uma data de prazo.

- Somente eventos ainda não iniciados podem ser reprogramados. A coluna Start time (Hora de início) do console e o campo NotBefore da AWS CLI indicam a hora de início do evento. Os eventos programados para início nos próximos cinco minutos não podem ser reprogramados.
- A nova hora de início do evento deve ser pelo menos 60 minutos a partir da hora atual.
- Se você reprogramar vários eventos usando o console, a data de prazo do evento será determinada pelo evento com a data de prazo do evento mais recente.

Definir janelas de eventos para eventos programados

Você pode definir janelas de eventos personalizadas recorrentes semanalmente para eventos agendados que reinicializam, interrompem ou terminam suas instâncias do Amazon EC2. É possível associar uma ou mais instâncias a uma janela de eventos. Se um evento agendado para essas instâncias estiver planejado, AWS irá programar os eventos dentro da janela de eventos associada.

Você pode usar janelas de eventos para maximizar a disponibilidade da workload especificando janelas de eventos que ocorrem durante períodos fora do pico para sua workload. Você também pode alinhar as janelas de eventos com suas programações de manutenção internas.

Você define uma janela de evento especificando um conjunto de intervalos de tempo. O intervalo de tempo mínimo é de duas horas. Os intervalos de tempo combinados devem totalizar pelo menos 4 horas.

Você pode associar uma ou mais instâncias a uma janela de evento usando IDs de instância ou tags de instância. Você também pode associar hosts dedicados a uma janela de evento usando o ID do host.

Warning

As janelas de eventos são aplicáveis apenas para eventos agendados que param, reinicializam ou encerram instâncias.

Janelas de eventos são não aplicável para:

- Eventos agendados e eventos de manutenção de rede acelerados.
- Manutenção não programada, como AutoRecovery e reinicializações não planejadas.

Trabalhar com janelas de eventos

- [Considerations \(p. 886\)](#)
- [Visualizador de eventos do Windows \(p. 887\)](#)
- [Criar janelas de eventos \(p. 889\)](#)
- [Modificar janelas de \(p. 892\)](#)
- [Excluir janelas de eventos \(p. 897\)](#)
- [Marcar janelas de eventos \(p. 897\)](#)

Considerations

- Todos os horários da janela de eventos são mostrados em UTC.
- A duração mínima da janela semanal de eventos é de quatro horas.
- Os intervalos de tempo dentro de uma janela de evento devem ser de pelo menos 2 horas.
- Apenas um tipo de destino (ID de instância, ID de host dedicado ou tag de instância) pode ser associado a uma janela de evento.
- Um destino (ID de instância, ID de host dedicado ou tag de instância) só pode ser associado a uma janela de evento.

- Um máximo de 100 IDs de instância, ou 50 IDs de host dedicados ou 50 tags de instância podem ser associados a uma janela de evento. As tags de instância podem ser associadas a qualquer número de instâncias.
- Um máximo de 200 janelas de eventos podem ser criadas por AWS Região :
- Várias instâncias associadas a janelas de eventos podem potencialmente ter eventos agendados ocorrem ao mesmo tempo.
- Se AWS já agendou um evento, modificar uma janela de evento não alterará a hora do evento agendado. Se o evento tiver uma data limite, você pode [reprogramar o evento \(p. 884\)](#).
- Você pode interromper e iniciar uma instância antes do evento agendado, que migra a instância para um novo host, e o evento agendado não ocorrerá mais.

Visualizador de eventos do Windows

É possível reagendar um evento usando um dos métodos a seguir.

Console

Para visualizar eventos usando o console do

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Selecione Ações, Gerenciar janelas de eventos.
4. Selecione uma janela de eventos para visualizar seus detalhes.

AWS CLI

Para descrever todas as janelas de eventos usando a AWS CLI

Usar o comando `aws describe-instance-event-windows`.

```
aws ec2 describe-instance-event-windows \
--region us-east-1
```

Saída esperada

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0abcdef1234567890",
            "Name": "myEventWindowName",
            "CronExpression": "* 21-23 * * 2,3",
            "AssociationTarget": {
                "InstanceIds": [
                    "i-1234567890abcdef0",
                    "i-0598c7d356eba48d7"
                ],
                "Tags": [],
                "DedicatedHostIds": []
            },
            "State": "active",
            "Tags": []
        }
    ...
}
```

```
    ],
    "NextToken": "9d624e0c-388b-4862-a31e-a85c64fc1d4a"
}
```

Para descrever uma janela de evento específica usando oAWS CLI

Usar [adescribe-instance-event-windows](#)com o comando--instance-event-window-idpara descrever uma janela de evento específica.

```
aws ec2 describe-instance-event-windows \
--region us-east-1 \
--instance-event-window-id iew-0abcdef1234567890
```

Para descrever as janelas de eventos que correspondam a um ou mais filtros usando oAWS CLI

Usar [adescribe-instance-event-windows](#)com o comando--filtersparâmetro . No exemplo a seguir, o filtro instance-id é usado para descrever todas as janelas de eventos que estão associadas à instância especificada.

Quando um filtro é usado, ele executa uma correspondência direta. No entanto, oinstance-ide diferente. Se não houver correspondência direta com o ID da instância, ele voltará para associações indiretas com a janela de eventos, como tags da instância ou ID de host dedicado (se a instância estiver em um host dedicado).

Para obter a lista de filtros compatíveis, consulte[describe-instance-event-windows](#)noAWS CLIRefência do.

```
aws ec2 describe-instance-event-windows \
--region us-east-1 \
--filters Name=instance-id,Values=i-1234567890abcdef0 \
--max-results 100 \
--next-token <next-token-value>
```

Saída esperada

No exemplo a seguir, a instância está em um Host Dedicado, que está associado à janela de evento.

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0dbc0adb66f235982",
            "TimeRanges": [
                {
                    "StartWeekDay": "sunday",
                    "StartHour": 2,
                    "EndWeekDay": "sunday",
                    "EndHour": 8
                }
            ],
            "Name": "myEventWindowName",
            "AssociationTarget": {
                "InstanceIds": [],
                "Tags": [],
                "DedicatedHostIds": [
                    "h-0140d9a7ecbd102dd"
                ]
            },
            "State": "active",
            "Tags": []
        }
    ]
}
```

]
}

Criar janelas de eventos

É possível criar uma ou mais janelas de eventos. Para cada janela de evento, você especifica um ou mais blocos de tempo. Por exemplo, é possível criar uma janela de evento com blocos de tempo que ocorrem todos os dias às 4h por duas horas. Ou você pode criar uma janela de evento com blocos de tempo que ocorrem aos domingos, das 2h às 4h, e às quartas-feiras, das 3h às 5h.

Para ver as restrições da janela de eventos, consulte [Considerations \(p. 886\)](#) Anteriormente neste tópico.

Janelas de eventos repetem semanalmente até que você as exclua.

Use um dos métodos a seguir para criar uma janela de eventos.

Console

Para criar uma regra para um evento do usando o console do

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Selecione Janela Criar evento de instância.
4. para oNome da janela de eventos, insira um nome descritivo para a janela de eventos.
5. para oAgendamentos de janelas, escolha especificar os blocos de tempo na janela de eventos usando o construtor de cron ou especificando intervalos de tempo.
 - Se escolher oConstrutor de cron, especifique o seguinte:
 1. para oDias (UTC), especifique os dias da semana em que a janela de eventos ocorre.
 2. para oHora de início (UTC), especifique a hora em que a janela de evento começa.
 3. para oDuration (Duração), especifique a duração dos blocos de tempo na janela do evento. A duração mínima por bloco de tempo é de 2 horas. A duração mínima da janela do evento deve ser igual ou superior a 4 horas no total. Todos os horários são em UTC.
 - Se escolher oIntervalos, escolha Adicione um novo intervalo de tempo e especifique o dia e a hora de início e o dia e a hora de término. Repita para cada intervalo de tempo. A duração mínima por intervalo de tempo é de 2 horas. A duração mínima para todos os intervalos de tempo combinados deve ser igual ou superior a 4 horas no total.
6. (Opcional) Para Detalhes do alvo, associe uma ou mais instâncias à janela de evento para que, se as instâncias estiverem agendadas para manutenção, o evento agendado ocorra durante a janela de evento associada. É possível associar uma ou mais instâncias a uma janela de evento usando IDs de instância ou tags de instância. É possível associar hosts dedicados a uma janela de evento usando o ID do host.
7. (Opcional) Para Tags da janela, escolha Adicionar tag(Opcional) e insira a chave e o valor da tag. Repita esse procedimento para cada tag.
8. Selecione Janela Criar eventos.

AWS CLI

Para criar uma janela de eventos usando a AWS CLI, crie primeiro a janela de evento e associe um ou mais destinos à janela de eventos.

Criar uma janela de eventos

Você pode definir um conjunto de intervalos de tempo ou uma expressão cron ao criar a janela de evento, mas não ambos.

Para criar uma janela de evento com um intervalo de tempo usando o AWS CLI

Usar `acreate-instance-event-window` especifique o `--time-range` parâmetro . Você também deve especificar o parâmetro `--cron-expression`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-window,Tags=[{Key=K1,Value=V1}]" \
    \
    --name myEventWindowName
```

Saída esperada

```
{ "InstanceEventWindow": { "InstanceId": "i-0abcdef1234567890", "TimeRanges": [ { "StartWeekDay": "monday", "StartHour": 2, "EndWeekDay": "wednesday", "EndHour": 8 } ], "Name": "myEventWindowName", "State": "creating", "Tags": [ { "Key": "K1", "Value": "V1" } ] } }
```

Para criar uma janela de evento com uma expressão cron usando o comando AWS CLI

Usar `acreate-instance-event-window` especifique o `--cron-expression` parâmetro . Você também deve especificar o parâmetro `--time-range`.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-window,Tags=[{Key=K1,Value=V1}]" \
    \
    --name myEventWindowName
```

Saída esperada

```
{ "InstanceEventWindow": { "InstanceId": "i-0abcdef1234567890", "Name": "myEventWindowName", }
```

```
"CronExpression": "* 21-23 * * 2,3",
"State": "creating",
"Tags": [
    {
        "Key": "K1",
        "Value": "V1"
    }
]
```

Associar um alvo a uma janela de evento

Você pode associar apenas um tipo de destino (IDs de instância, IDs de host dedicado ou tags de instância) a uma janela de evento.

Para associar tags de instância a uma janela de evento usando oAWS CLI

Usar `aassociar-instance-event-window` especifique `oinstance-event-window-id`parâmetro para especificar a janela de evento. Para associar tags de instância, especifique `o--association-target` para os valores de parâmetro, especifique uma ou mais tags.

```
aws ec2 associate-instance-event-window \
--region us-east-1 \
--instance-event-window-id iew-0abcdef1234567890 \
--association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Para associar uma ou mais instâncias a uma janela de evento usando oAWS CLI

Usar `aassociar-instance-event-window` especifique `oinstance-event-window-id`parâmetro para especificar a janela de evento. Para associar instâncias, especifique `o--association-target` para os valores de parâmetro, especifique um ou mais IDs de instância.

```
aws ec2 associate-instance-event-window \
--region us-east-1 \
```

```
--instance-event-window-id iew-0abcdef1234567890 \
--association-target "InstanceIds=i-1234567890abcdef0, i-0598c7d356eba48d7"
```

Saída esperada

```
{  
    "InstanceEventWindow": {  
        "InstanceEventWindowId": "iew-0abcdef1234567890",  
        "Name": "myEventWindowName",  
        "CronExpression": "* 21-23 * * 2,3",  
        "AssociationTarget": {  
            "InstanceIds": [  
                "i-1234567890abcdef0",  
                "i-0598c7d356eba48d7"  
            ],  
            "Tags": [],  
            "DedicatedHostIds": []  
        },  
        "State": "creating"  
    }  
}
```

Para associar um Host Dedicado a uma janela de evento usando o AWS CLI

Usar `aassociar-instance-event-window` especifique o `instance-event-window-id` parâmetro para especificar a janela de evento. Para associar um Host Dedicado, especifique o `--association-target`, para os valores de parâmetro, especifique um ou mais IDs de Host Dedicado.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Saída esperada

```
{  
    "InstanceEventWindow": {  
        "InstanceEventWindowId": "iew-0abcdef1234567890",  
        "Name": "myEventWindowName",  
        "CronExpression": "* 21-23 * * 2,3",  
        "AssociationTarget": {  
            "InstanceIds": [],  
            "Tags": [],  
            "DedicatedHostIds": [  
                "h-029fa35a02b99801d"  
            ]  
        },  
        "State": "creating"  
    }  
}
```

Modificar janelas de

É possível modificar todos os campos de uma janela de evento, exceto seu ID. Por exemplo, quando o horário de verão começar, convém modificar o agendamento da janela de eventos. Para janelas de eventos existentes, talvez você queira adicionar ou remover destinos.

Para modificar um volume do EBS, use um dos métodos a seguir.

Console

Para modificar uma janela de eventos usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Selecione Ações, Gerenciar janelas de eventos.
4. Selecione a janela de eventos a ser modificada e escolha Ações, Janela Modificar evento da.
5. Modifique os campos na janela de eventos e escolha Modify event window.

AWS CLI

Para modificar uma janela de eventos usando o AWS CLI, você pode modificar o intervalo de tempo ou a expressão cron e associar ou desassociar um ou mais destinos à janela de evento.

Modificar a hora da janela de

Você pode modificar um intervalo de tempo ou uma expressão cron ao modificar a janela de evento, mas não ambos.

Para modificar o intervalo de tempo de uma janela de evento usando o AWS CLI

Usar a `aws ec2 modify-instance-event-window` especifica a janela de evento a ser modificada. Especifique o `--time-range` parâmetro para modificar o intervalo de tempo. Você também deve especificar o parâmetro `--cron-expression`.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

```
        }
    }
}
```

Para modificar um conjunto de intervalos de tempo para uma janela de evento usando o AWS CLI

Usar a [aws modify-instance-event-window](#) especifique a janela de evento a ser modificada. Especifique o `--time-range` Parâmetro para modificar o intervalo de tempo. Você também não pode especificar o `--cron-expression` Parâmetro na mesma chamada.

```
aws ec2 modify-instance-event-window \
--region us-east-1 \
--instance-event-window-id iew-0abcdef1234567890 \
--time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay": "wednesday", "EndHour": 8},
 {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday", "EndHour": 8}]'
```

Saída esperada

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Para modificar a expressão cron de uma janela de evento usando o comando AWS CLI

Usar a [aws modify-instance-event-window](#) especifique a janela de evento a ser modificada. Especifique o `--cron-expression` para modificar a expressão cron. Você também deve especificar o parâmetro `--time-range`.

```
aws ec2 modify-instance-event-window \
--region us-east-1 \
--instance-event-window-id iew-0abcdef1234567890 \
--cron-expression "* 21-23 * * 2,3"
```

Saída esperada

```
{  
    "InstanceEventWindow": {  
        "InstanceEventWindowId": "iew-0abcdef1234567890",  
        "Name": "myEventWindowName",  
        "CronExpression": "* 21-23 * * 2,3",  
        "AssociationTarget": {  
            "InstanceIds": [  
                "i-0abcdef1234567890",  
                "i-0be35f9acb8ba01f0"  
            ],  
            "Tags": [],  
            "DedicatedHostIds": []  
        },  
        "State": "creating",  
        "Tags": [  
            {  
                "Key": "K1",  
                "Value": "V1"  
            }  
        ]  
    }  
}
```

Modificar os alvos associados a uma janela de evento

Você pode associar alvos adicionais a uma janela de evento. Você também pode desassociar alvos existentes de uma janela de evento. No entanto, apenas um tipo de destino (IDs de instância, IDs de host dedicado ou tags de instância) pode ser associado a uma janela de evento.

Para associar alvos adicionais a uma janela de evento

Para obter instruções sobre como associar alvos a uma janela de evento, consulte [Associate a target with an event window](#).

Para desassociar tags de instância de uma janela de evento usando o AWS CLI

Usar `aws ec2 disassociate-instance-event-janela` e especifique o `instance-event-window-id` parâmetro para especificar a janela de evento. Para desassociar tags de instância, especifique o `--association-target` para os valores de parâmetro, especifique uma ou mais tags.

```
aws ec2 disassociate-instance-event-window \
--region us-east-1 \
--instance-event-window-id iew-0abcdef1234567890 \
--association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Saída esperada

```
{  
    "InstanceEventWindow": {  
        "InstanceEventWindowId": "iew-0abcdef1234567890",  
        "Name": "myEventWindowName",  
        "CronExpression": "* 21-23 * * 2,3",  
        "AssociationTarget": {  
            "InstanceIds": [  
                "i-0abcdef1234567890",  
                "i-0be35f9acb8ba01f0"  
            ],  
            "Tags": [],  
            "DedicatedHostIds": []  
        }  
    }  
}
```

```
        "AssociationTarget": {  
            "InstanceIds": [],  
            "Tags": [],  
            "DedicatedHostIds": []  
        },  
        "State": "creating"  
    }  
}
```

Para desassociar uma ou mais instâncias de uma janela de evento usando oAWS CLI

Usar [adisassociar-instance-event-janela](#) e especifique o[instance-event-window-id](#)parâmetro para especificar a janela de evento. Para desassociar instâncias, especifique o--association-target para os valores de parâmetro, especifique um ou mais IDs de instância.

```
aws ec2 disassociate-instance-event-window \  
    --region us-east-1 \  
    --instance-event-window-id iew-0abcdef1234567890 \  
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Saída esperada

```
{  
    "InstanceEventWindow": {  
        "InstanceEventWindowId": "iew-0abcdef1234567890",  
        "Name": "myEventWindowName",  
        "CronExpression": "* 21-23 * * 2,3",  
        "AssociationTarget": {  
            "InstanceIds": [],  
            "Tags": [],  
            "DedicatedHostIds": []  
        },  
        "State": "creating"  
    }  
}
```

Para desassociar um Host Dedicado de uma janela de evento usando oAWS CLI

Usar [adisassociar-instance-event-janela](#) e especifique o[instance-event-window-id](#)parâmetro para especificar a janela de evento. Para desassociar um Host Dedicado, especifique o--association-target, para os valores de parâmetro, especifique um ou mais IDs de Host Dedicado.

```
aws ec2 disassociate-instance-event-window \  
    --region us-east-1 \  
    --instance-event-window-id iew-0abcdef1234567890 \  
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Saída esperada

```
{  
    "InstanceEventWindow": {  
        "InstanceEventWindowId": "iew-0abcdef1234567890",  
        "Name": "myEventWindowName",  
        "CronExpression": "* 21-23 * * 2,3",  
        "AssociationTarget": {  
            "InstanceIds": [],  
            "Tags": [],  
            "DedicatedHostIds": []  
        }  
    }  
}
```

```
    },
    "State": "creating"
}
```

Excluir janelas de eventos

É possível excluir uma janela de eventos de cada vez usando um dos métodos a seguir.

Console

Para excluir uma janela de eventos usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Selecione Ações, Gerenciar janelas de eventos.
4. Selecione a janela de eventos a ser excluída e escolha Ações, Janela de evento Excluir instância.
5. Quando solicitado, digite **delete** e escolha Delete (Excluir).

AWS CLI

Para excluir uma janela de eventos usando o AWS CLI

Usar `aws ec2 delete-instance-event-window` especifique a janela de evento a ser excluída.

```
aws ec2 delete-instance-event-window \
--region us-east-1 \
--instance-event-window-id iew-0abcdef1234567890
```

Para forçar a exclusão de uma janela de evento usando o AWS CLI

Usar `--force-delete` se a janela de evento estiver atualmente associada a destinos.

```
aws ec2 delete-instance-event-window \
--region us-east-1 \
--instance-event-window-id iew-0abcdef1234567890 \
--force-delete
```

Saída esperada

```
{
  "InstanceEventWindowState": {
    "InstanceEventWindowId": "iew-0abcdef1234567890",
    "State": "deleting"
  }
}
```

Marcar janelas de eventos

Você pode marcar uma janela de evento ao criá-la ou posteriormente.

Para marcar uma janela de evento ao criá-la, consulte [Criar janelas de eventos \(p. 889\)](#).

Use um dos métodos a seguir para marcar uma janela de evento.

Console

Como marcar uma existente usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events.
3. Selecione Ações, Gerenciar janelas de eventos.
4. Selecione a janela de eventos a ser marcada e escolha Ações, Gerenciar tags de janela de evento de.
5. Para adicionar uma tag, escolha Add tag. Repita esse procedimento para cada tag.
6. Escolha Save (Salvar).

AWS CLI

Para marcar uma janela de evento existente usando o AWS CLI

Use o comando [create-tags](#) para marcar os recursos existentes. No exemplo a seguir, a solicitação de existente é marcada com Key=purpose e Value=test.

```
aws ec2 create-tags \
    --resources iew-0abcdef1234567890 \
    --tags Key=purpose,Value=test
```

Monitorar instâncias usando o CloudWatch

Você pode monitorar suas instâncias usando o Amazon CloudWatch, que coleta e processa os dados brutos do Amazon EC2 em métricas legíveis, quase em tempo real. Essas estatísticas são registradas para um período de 15 meses, de forma que você possa acessar informações históricas e ganhar uma perspectiva melhor sobre como seu serviço ou aplicação Web está se saindo.

Por padrão, o Amazon EC2 envia dados de métrica ao CloudWatch em períodos de 5 minutos. Para enviar dados de métrica para sua instância ao CloudWatch em períodos de 1 minuto, você pode habilitar o monitoramento detalhado na instância. Para obter mais informações, consulte [Habilitar ou desabilitar o monitoramento detalhado para instâncias \(p. 899\)](#).

O console do Amazon EC2 exibe uma série de gráficos com base nos dados brutos do Amazon CloudWatch. Dependendo de suas necessidades, você pode preferir obter dados para suas instâncias do Amazon CloudWatch em vez de gráficos no console.

Para obter mais informações sobre o Amazon CloudWatch, consulte o [Guia do usuário do Amazon CloudWatch](#).

Tópicos

- [Habilitar ou desabilitar o monitoramento detalhado para instâncias \(p. 899\)](#)
- [Listar as métricas disponíveis do CloudWatch para as instâncias \(p. 901\)](#)
- [Obter estatísticas para as métricas das instâncias \(p. 914\)](#)
- [Representar métricas em gráficos para as instâncias \(p. 922\)](#)
- [Criar um alarme do CloudWatch para uma instância \(p. 922\)](#)
- [Criar alarmes para interromper, encerrar, reiniciar ou recuperar uma instância \(p. 924\)](#)

Habilitar ou desabilitar o monitoramento detalhado para instâncias

Por padrão, sua instância está habilitada para monitoramento básico. Você também pode habilitar o monitoramento detalhado. Depois de habilitar o monitoramento detalhado, o console do Amazon EC2 exibirá gráficos de monitoramento com um período de 1 minuto para a instância.

Veja a seguir a descrição do intervalo de dados e a cobrança para o monitoramento básico e detalhado de instâncias.

Tipo de monitoramento	Descrição	Cobranças
Monitoramento básico	Os dados são disponibilizados automaticamente em períodos de cinco minutos.	Sem cobrança
Monitoramento detalhado	Os dados estão disponíveis em períodos de um minuto. Para obter esse nível de dados, você deve especificamente habilitá-lo para a instância. Para as instâncias onde você tiver habilitado monitoramento detalhado, você também pode obter dados agregados nos grupos de instâncias semelhantes.	A cobrança é feita por métrica enviada ao CloudWatch. Você não é cobrado pelo armazenamento de dados. Para obter mais informações, consulte Nível pago e Exemplo 1 – Monitoramento detalhado do EC2 na página de definição de preço de Amazon CloudWatch .

Tópicos

- [Permissões obrigatórias do IAM \(p. 899\)](#)
- [Habilitar o monitoramento detalhado \(p. 899\)](#)
- [Desativar o monitoramento detalhado \(p. 900\)](#)

Permissões obrigatórias do IAM

Para habilitar o monitoramento detalhado de uma instância, o usuário do IAM deve ter permissão para usar a ação da API [MonitorInstances](#). Para desabilitar o monitoramento detalhado de uma instância, o usuário do IAM deve ter permissão para usar a ação da API [UnmonitorInstances](#).

Habilitar o monitoramento detalhado

Você pode habilitar o monitoramento detalhado em uma instância quando a executá-la ou depois de a instância estiver sendo executada ou interrompida. Habilitar o monitoramento detalhado em uma instância não afeta o monitoramento dos volumes do EBS anexados à instância. Para obter mais informações, consulte [Métricas do Amazon CloudWatch para o Amazon EBS \(p. 1472\)](#).

New console

Para habilitar o monitoramento detalhado para uma instância existente

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitoring (Monitoramento), Manage detailed monitoring (Gerenciar monitoramento detalhado).

4. Na página de detalhes Detailed monitoring (Monitoramento detalhado), em Detailed monitoring (Monitoramento detalhado), marque a caixa de seleção Enable (Habilitar).
5. Escolha Save (Salvar).

Para habilitar o monitoramento detalhado ao executar uma instância

Ao executar uma instância usando o AWS Management Console, selecione a caixa Monitoring (Monitoramento) na página Configure Instance Details (Configurar detalhes de instância).

Old console

Para habilitar o monitoramento detalhado para uma instância existente

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), CloudWatch Monitoring (Monitoramento do CloudWatch), Enable Detailed Monitoring (Habilitar monitoramento detalhado).
4. Na caixa de diálogo Enable Detailed Monitoring (Habilitar monitoramento detalhado), escolha Yes, Enable (Sim, habilitar).
5. Escolha Close (Fechar).

Para habilitar o monitoramento detalhado ao executar uma instância (console)

Ao executar uma instância usando o AWS Management Console, selecione a caixa Monitoring (Monitoramento) na página Configure Instance Details (Configurar detalhes de instância).

AWS CLI

Para habilitar o monitoramento detalhado para uma instância existente

Use o comando `monitor-instances` para habilitar o monitoramento detalhado das instâncias especificadas.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Para habilitar o monitoramento detalhado ao executar uma instância

Use o comando `run-instances` com o marcador `--monitoring` para ativar o monitoramento detalhado.

```
aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

Desativar o monitoramento detalhado

Você pode desativar o monitoramento detalhado em uma instância quando executá-la ou depois de a instância estar sendo executada ou ter sido interrompida.

New console

Para desabilitar o monitoramento detalhado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitoring (Monitoramento), Manage detailed monitoring (Gerenciar monitoramento detalhado).

4. Na página de detalhes Detailed monitoring (Monitoramento detalhado), em Detailed monitoring (Monitoramento detalhado), desmarque a caixa de seleção Enable (Habilitar).
5. Escolha Save (Salvar).

Old console

Para desabilitar o monitoramento detalhado

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), CloudWatch Monitoring (Monitoramento do CloudWatch), Disable Detailed Monitoring (Desabilitar monitoramento detalhado).
4. Na caixa de diálogo Disable Detailed Monitoring (Desabilitar monitoramento detalhado), escolha Yes, Disable (Sim, desabilitar).
5. Escolha Close (Fechar).

AWS CLI

Para desabilitar o monitoramento detalhado

Use o comando `unmonitor-instances` para desativar o monitoramento detalhado das instâncias especificadas.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

Listar as métricas disponíveis do CloudWatch para as instâncias

O Amazon EC2 envia métricas para o Amazon CloudWatch. Você pode usar o AWS Management Console, a AWS CLI ou uma API para listar as métricas que o Amazon EC2 envia para o CloudWatch. Por padrão, cada ponto de dados abrange os 5 minutos seguintes ao início da atividade para a instância. Se você tiver habilitado o monitoramento detalhado, cada ponto de dados abrangerá o minuto seguinte ao início da atividade. Observe que, para as estatísticas Mínimo, Máximo e Média, a granularidade mínima para as métricas que o EC2 fornece é de 1 minuto.

Para obter informações sobre a obtenção de estatísticas para essas métricas, consulte [Obter estatísticas para as métricas das instâncias \(p. 914\)](#).

Tópicos

- [Métricas de instância \(p. 902\)](#)
- [Métricas de crédito de CPU \(p. 904\)](#)
- [Métricas de Host Dedicado \(p. 906\)](#)
- [Métricas do Amazon EBS para instâncias baseadas em Nitro \(p. 906\)](#)
- [Métricas de verificação de status \(p. 908\)](#)
- [Métricas de espelhamento de tráfego \(p. 909\)](#)
- [Dimensões de métrica do Amazon EC2 \(p. 909\)](#)
- [Métricas de uso do Amazon EC2 \(p. 910\)](#)
- [Listar métricas usando o console \(p. 911\)](#)
- [Listar métricas usando o AWS CLI \(p. 913\)](#)

Métricas de instância

O namespace AWS/EC2 inclui as métricas de instância a seguir.

Métrica	Descrição
CPUUtilization	<p>O percentual de unidades alocadas de computação EC2 que estão sendo utilizadas na instância no momento. Essa métrica identifica o poder de processamento necessário para executar uma aplicação em uma instância selecionada.</p> <p>Dependendo do tipo de instância, ferramentas em seu sistema operacional podem exibir um percentual mais baixo do que CloudWatch quando a instância não alocar um núcleo do processador.</p> <p>Unidades: percentual</p>
DiskReadOps	<p>Operações de leitura concluídas de todos os volumes de armazenamento de instâncias disponíveis para a instância em um período de tempo especificado.</p> <p>Para calcular a média de operações de I/O por segundo (IOPS) para o período, divida o total das operações pelo número de segundos no período em questão.</p> <p>Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.</p> <p>Unidades: contagem</p>
DiskWriteOps	<p>Operações de gravação concluídas em todos os volumes de armazenamento de instâncias disponíveis para a instância em um período de tempo especificado.</p> <p>Para calcular a média de operações de I/O por segundo (IOPS) para o período, divida o total das operações pelo número de segundos no período em questão.</p> <p>Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.</p> <p>Unidades: contagem</p>
DiskReadBytes	<p>Bytes lidos de todos os volumes de armazenamento de instâncias disponíveis para a instância.</p> <p>Essa métrica é utilizada para determinar o volume de dados que a aplicação lê do disco rígido da instância. Isso pode ser usado para determinar a velocidade da aplicação.</p> <p>O número relatado é o número de bytes recebidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60.</p> <p>Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.</p>

Métrica	Descrição
	Unidades: bytes
DiskWriteBytes	<p>Bytes gravados em todos os volumes de armazenamento de instâncias disponíveis para a instância.</p> <p>Essa métrica é utilizada para determinar o volume de dados que a aplicação grava no disco rígido da instância. Isso pode ser usado para determinar a velocidade do aplicativo.</p> <p>O número relatado é o número de bytes recebidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60.</p> <p>Se não houver nenhum volume de armazenamento de instâncias, o valor será 0 ou a métrica não será relatada.</p> <p>Unidades: bytes</p>
MetadataNoToken	<p>O número de vezes que o serviço de metadados da instância foi acessado com êxito usando um método que não use um token.</p> <p>Essa métrica é usada para determinar se existem processos que acessam metadados de instância que usam Serviço de metadados da instância versão 1, que não usa um token. Se todas as solicitações usarem sessões baseadas em tokens, por exemplo Serviço de metadados da instância versão 2, o valor será 0. Para obter mais informações, consulte Transição para usar o Serviço de metadados da instância versão 2 (p. 625).</p> <p>Unidades: contagem</p>
NetworkIn	<p>A quantidade de bytes recebidos em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de rede de entrada para uma única instância.</p> <p>O número relatado é o número de bytes recebidos durante o período. Se você estiver usando o monitoramento básico (5 minutos) e a estatística for Sum (Soma), divida esse número por 300 para encontrar o número de bytes/segundo. Se você tiver o monitoramento detalhado (1 minuto) e a estatística for Sum (soma), divida o número por 60.</p> <p>Unidade: bytes</p>

Métrica	Descrição
<code>NetworkOut</code>	<p>A quantidade de bytes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de rede de saída de uma única instância.</p> <p>O número relatado é o número de bytes enviados durante o período. Se você estiver usando o monitoramento básico (5 minutos) e a estatística for Sum (Soma), divida esse número por 300 para encontrar o número de bytes/segundo. Se você tiver o monitoramento detalhado (1 minuto) e a estatística for Sum (soma), divida o número por 60.</p> <p>Unidade: bytes</p>
<code>NetworkPacketsIn</code>	<p>A quantidade de pacotes recebidos em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de entrada em termos do número de pacotes em uma única instância.</p> <p>Essa métrica está disponível apenas para monitoramento básico (períodos de 5 minutos). Para calcular a quantidade de pacotes por segundo (PPS) que sua instância recebeu nos 5 minutos, divida o valor da estatística Sum (soma) por 300.</p> <p>Unidade: contagem</p>
<code>NetworkPacketsOut</code>	<p>A quantidade de pacotes enviados em todas as interfaces de rede pela instância. Essa métrica identifica o volume de tráfego de saída em termos do número de pacotes em uma única instância.</p> <p>Essa métrica está disponível apenas para monitoramento básico (períodos de 5 minutos). Para calcular a quantidade de pacotes por segundo (PPS) que sua instância recebeu nos 5 minutos, divida o valor da estatística Sum (soma) por 300.</p> <p>Unidade: contagem</p>

Métricas de crédito de CPU

O namespace AWS/EC2 inclui as seguintes métricas de crédito de CPU para suas [instâncias expansíveis](#) (p. 169).

Métrica	Descrição
<code>CPUCreditUsage</code>	<p>O número de créditos de CPU gastos pela instância por utilização de CPU. Um crédito de CPU equivale a um vCPU em execução em 100% de utilização por um minuto ou a uma combinação equivalente de vCPUs, utilização e tempo (por exemplo, um vCPU em execução a 50% de utilização por dois minutos ou dois vCPUs em execução a 25% de utilização por dois minutos).</p> <p>As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos. Se você especificar um período de mais cinco minutos, use a estatística <code>Sum</code> em vez da estatística <code>Average</code>.</p> <p>Unidades: créditos (minutos de vCPU)</p>

Métrica	Descrição
CPUCreditBalance	<p>O número de créditos ganhos de CPU que uma instância acumulou desde que foi executada ou iniciada. Para a T2 Padrão, o CPUCreditBalance também inclui o número de créditos de execução que foram acumulados.</p> <p>Os créditos são acumulados no saldo de créditos após terem sido ganhos e são removidos do saldo de créditos quando são gastos. O saldo de crédito tem um limite máximo, determinado pelo tamanho da instância. Depois que o limite for atingido, todos os novos créditos ganhos serão descartados. Para a T2 Padrão, os créditos de execução não são contabilizados para o limite.</p> <p>Os créditos do CPUCreditBalance são disponibilizados para que a instância gaste e apresente intermitência com uma utilização de CPU acima da linha de base.</p> <p>Quando uma instância está em execução, os créditos do CPUCreditBalance não expiram. Quando uma instância T3 ou T3a é interrompida, o valor CPUCreditBalance persiste por sete dias. Consequentemente, todos os créditos acumulados são perdidos. Quando uma instância T2 é interrompida, o valor CPUCreditBalance não persiste, e todos os créditos acumulados são perdidos.</p> <p>As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos.</p> <p>Unidades: créditos (minutos de vCPU)</p>
CPUSurplusCreditBalance	<p>O número de créditos excedentes gastos por uma instância <code>unlimited</code> quando seu valor CPUCreditBalance é zero.</p> <p>O valor CPUSurplusCreditBalance é pago pelos créditos de CPU ganhos. Se o número de créditos excedentes ultrapassar o número máximo de créditos que a instância pode ganhar em um período de 24 horas, os créditos excedentes gastos acima do limite máximo incorrerão em uma taxa adicional.</p> <p>As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos.</p> <p>Unidades: créditos (minutos de vCPU)</p>

Métrica	Descrição
CPUSurplusCreditsCharged	<p>O número de créditos excedentes gastos que não são pagos pelos créditos de CPU ganhos e que, portanto, incorrem em uma cobrança adicional.</p> <p>Os créditos excedentes gastos são cobrados quando uma das seguintes situações ocorre:</p> <ul style="list-style-type: none">• Os créditos excedentes ultrapassaram o número máximo de créditos que a instância pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora.• A instância é interrompida ou encerrada.• A instância é alterada de <code>unlimited</code> para <code>standard</code>. <p>As métricas de crédito de CPU estão disponíveis apenas a uma frequência de 5 minutos.</p> <p>Unidades: créditos (minutos de vCPU)</p>

Métricas de Host Dedicado

O namespace AWS/EC2 inclui as métricas a seguir para hosts dedicados T3.

Métrica	Descrição
DedicatedHostCPUUtilization	A porcentagem de capacidade computacional alocada que está atualmente em uso pelas instâncias em execução no Host Dedicado. Unidade: percentual

Métricas do Amazon EBS para instâncias baseadas em Nitro

O namespace AWS/EC2 inclui as seguintes métricas do Amazon EBS para as instâncias baseadas em Nitro que não são instâncias bare metal. Para obter a lista de tipos de instância baseadas em Nitro, consulte [Instâncias criadas no Sistema Nitro \(p. 154\)](#).

Os valores das métricas de instâncias baseadas em Nitro sempre serão inteiros (números inteiros), enquanto os valores de instâncias baseadas em Xen oferecem suporte a decimais. Portanto, a utilização baixa de CPU de instâncias baseadas em Nitro pode ser exibida arredondada para 0.

Métrica	Descrição
EBSReadOps	Operações de leitura concluídas de todos os volumes do Amazon EBS anexados à instância em um período especificado. Para calcular a média de operações de E/S de leitura por segundo (IOPS de leitura) para o período, divida o total das operações pelo número de segundos no período em questão. Se você estiver usando o monitoramento básico

Métrica	Descrição
	(5 minutos), divida esse número por 300 para calcular IOPS de leitura. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Unidade: contagem
EBSWriteOps	Operações de gravação concluídas para todos os volumes do EBS anexados à instância em um período especificado. Para calcular a média de operações de E/S de gravação por segundo (IOPS de gravação) para o período, divida o total das operações pelo número de segundos no período em questão. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para calcular o IOPS de gravação. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Unidade: contagem
EBSReadBytes	Bytes lidos de todos os volumes do EBS anexados à instância em um período especificado. O número relatado é o número de bytes lidos durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes lidos/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Unidade: bytes
EBSWriteBytes	Bytes gravados em todos os volumes do EBS anexados à instância em um período especificado. O número relatado é o número de bytes gravados durante o período. Se você estiver usando o monitoramento básico (5 minutos), divida esse número por 300 para encontrar o número de bytes gravados/segundo. Se você estiver usando o monitoramento detalhado (1 minuto), divida o número por 60. Unidade: bytes

Métrica	Descrição
EBSIOBalance%	<p>Fornece informações sobre a porcentagem de créditos de E/S restantes no bucket de intermitência. Essa métrica está disponível somente para monitoramento básico.</p> <p>Os tamanhos de instância que oferecem suporte a essa métrica podem ser encontrados na tabela em Otimizadas para EBS por padrão (p. 1441): as instâncias na coluna Instance size (Tamanho da instância) que incluem um asterisco (*) oferecem suporte a essa métrica.</p> <p>A estatística Sum não é aplicável a essa métrica.</p> <p>Unidade: percentual</p>
EBSByteBalance%	<p>Fornece informações sobre a porcentagem de créditos de transferência restantes no bucket de intermitência. Essa métrica está disponível somente para monitoramento básico.</p> <p>Os tamanhos de instância que oferecem suporte a essa métrica podem ser encontrados na tabela em Otimizadas para EBS por padrão (p. 1441): as instâncias na coluna Instance size (Tamanho da instância) que incluem um asterisco (*) oferecem suporte a essa métrica.</p> <p>A estatística Sum não é aplicável a essa métrica.</p> <p>Unidade: percentual</p>

Para obter informações sobre as métricas fornecidas para seus volumes do EBS, consulte [Métricas do Amazon EBS \(p. 1473\)](#). Para obter informações sobre as métricas fornecidas para suas frotas Spot, consulte [Métricas do CloudWatch para frota spot \(p. 790\)](#).

Métricas de verificação de status

O namespace AWS/EC2 inclui as métricas de verificação de status a seguir. Por padrão, as métricas de verificação de status estão disponíveis a uma frequência de um minuto gratuitamente. Para uma instância recém-executada, os dados de métrica de verificação de status só estarão disponíveis após a instância ter concluído o estado de inicialização (alguns minutos depois de a instância entrar no estado de execução). Para obter mais informações sobre verificações de status do EC2, consulte [Verificações de status para as instâncias \(p. 867\)](#).

Métrica	Descrição
StatusCheckFailed	<p>Relata se a instância foi aprovada tanto na verificação do status da instância quanto na verificação do status do sistema no último minuto.</p> <p>Essa métrica pode ser 0 (passou) ou 1 (falhou).</p> <p>Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.</p> <p>Unidades: contagem</p>

Métrica	Descrição
StatusCheckFailed_Instance	<p>Informa se a instância foi aprovada na verificação de status de instância no último minuto.</p> <p>Essa métrica pode ser 0 (passou) ou 1 (falhou).</p> <p>Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.</p> <p>Unidades: contagem</p>
StatusCheckFailed_System	<p>Informa se a instância foi aprovada na verificação de status de sistema do & no último minuto.</p> <p>Essa métrica pode ser 0 (passou) ou 1 (falhou).</p> <p>Por padrão, esta métrica está disponível a uma frequência de um minuto gratuitamente.</p> <p>Unidades: contagem</p>

Métricas de espelhamento de tráfego

O namespace AWS/EC2 inclui métricas para tráfego espelhado. Para obter mais informações, consulte [Monitorar o tráfego espelhado usando o Amazon CloudWatch](#) no Guia de espelhamento de tráfego da Amazon VPC.

Dimensões de métrica do Amazon EC2

Você pode usar as seguintes dimensões para refinar as métricas listadas nas tabelas anteriores.

Dimensão	Descrição
AutoScalingGroupName	Essa dimensão filtra os dados solicitados para todas as instâncias em um grupo de capacidade especificado. Um Grupo de Auto Scaling é uma coleção de instâncias que você define se estiver usando o Auto Scaling. Essa dimensão está disponível somente para métricas do Amazon EC2 quando as instâncias estão em um grupo de Auto Scaling. Disponível para instâncias com monitoramento básico ou detalhado habilitado.
ImageId	Essa dimensão filtra os dados que você solicita para todas as instâncias executando essa Imagem de máquina da Amazon (AMI) do Amazon EC2. Disponível para instâncias com monitoramento detalhado habilitado.
InstanceId	Essa dimensão filtra os dados que você solicita somente para a instância identificada. Isso ajuda você a identificar uma instância exata para monitorar os dados.
InstanceType	Essa dimensão filtra os dados que você solicita para todas as instâncias executando esse tipo de instância especificado. Isso ajuda você a categorizar seus dados pelo tipo de instância em execução. Por exemplo, você pode comparar dados de uma instância m1.small e uma instância m1.large para determinar qual delas tem o melhor

Dimensão	Descrição
	valor comercial para sua aplicação. Disponível para instâncias com monitoramento detalhado habilitado.

Métricas de uso do Amazon EC2

Você pode usar métricas de uso do CloudWatch para fornecer visibilidade sobre o uso de recursos de sua conta. Use essas métricas para visualizar o uso do serviço atual nos gráficos e painéis do CloudWatch.

As métricas de uso do Amazon EC2 correspondem às cotas de serviço da AWS. Também é possível configurar alarmes que alertem você quando o uso se aproximar de uma cota de serviço. Para obter mais informações sobre a integração do CloudWatch com cotas de serviço, consulte [Métricas de integração e uso de cotas de serviço](#).

O Amazon EC2 publica as seguintes métricas no namespace AWS/Usage.

Métrica	Descrição
ResourceCount	O número dos recursos especificados em execução em sua conta. Os recursos são definidos pelas dimensões associadas à métrica. A estatística mais útil para essa métrica é MAXIMUM, que representa o número máximo de recursos usados durante o período de um minuto.

As dimensões a seguir são usadas para refinar as métricas de uso publicadas pelo Amazon EC2.

Dimensão	Descrição
Service	O nome do serviço da AWS que contém o recurso. Para as métricas de uso do Amazon EC2, o valor dessa dimensão é EC2.
Type	O tipo de entidade que está sendo relatado. Atualmente, o único valor válido para métricas de uso do Amazon EC2 é Resource.
Resource	O tipo de recurso que está em execução. Atualmente, o único valor válido para métricas de uso do Amazon EC2 é vCPU, que retorna informações sobre as instâncias em execução.
Class	A classe do recurso que está sendo acompanhado. Para as métricas de uso do Amazon EC2 com vCPU como o valor da dimensão Resource, os valores válidos são Standard/OnDemand, F/OnDemand, G/OnDemand, Inf/OnDemand, P/OnDemand e X/OnDemand. Os valores dessa dimensão definem a primeira letra dos tipos de instância relatados pela métrica. Por exemplo, Standard/OnDemand retorna informações sobre todas as instâncias em execução com tipos que começam com A, C, D, H, I, M, R, T e Z, e G/OnDemand retorna informações sobre todas as instâncias em execução com tipos que começam com G.

Listar métricas usando o console

As métricas são agrupadas primeiro pelo namespace e, em seguida, por várias combinações de dimensão dentro de cada namespace. Por exemplo, você pode ver todas as métricas fornecidas pelo Amazon EC2 ou as métricas agrupadas por ID de instância, tipo de instância, ID da imagem (AMI) ou grupo do Auto Scaling.

Para exibir as métricas disponíveis por categoria (console)

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace de métricas do EC2.

The screenshot shows the AWS CloudWatch Metrics console interface. At the top, there are three tabs: 'All metrics' (highlighted in orange), 'Graphed metrics', and 'Graph options'. Below the tabs is a search bar with the placeholder text 'Search for any metric, dimension or resource id'. The main area displays a grid of service namespaces with their metric counts:

Service Namespace	Number of Metrics
EBS	117 Metrics
EC2	316 Metrics
EFS	7 Metrics
ELB	210 Metrics
ElasticBeanstalk	8 Metrics
RDS	60 Metrics
S3	4 Metrics

4. Selecione uma dimensão de métrica (por exemplo, Per-Instance Metrics (Métricas por instância)).

The screenshot shows the AWS CloudWatch Metrics console with the following interface elements:

- Top navigation bar with tabs: All metrics, Graphed metrics, Graph options.
- Breadcrumbs: All > EC2.
- Search bar: Search for any metric, dimension or resource id.
- Main title: 103 Metrics.
- Category cards:
 - By Auto Scaling Group: 28 Metrics
 - By Image (AMI) Id: 7 Metrics
 - Per-Instance Metrics: 54 Metrics
 - Aggregated by Instance Type: 7 Metrics
 - Across All Instances: 7 Metrics

5. Para classificar a métrica, use o cabeçalho da coluna. Para criar um gráfico de uma métrica, marque a caixa de seleção ao lado da métrica. Para filtrar por recurso, escolha o ID do recurso e, em seguida, escolha Add to search (Adicionar à pesquisa). Para filtrar por métrica, selecione o nome da métrica e, em seguida, escolha Add to search (Adicionar à pesquisa).

The screenshot shows the AWS CloudWatch Metrics console with the following interface elements:

- Top navigation bar with tabs: All metrics, Graphed metrics, Graph options.
- Breadcrumbs: All > EC2 > Per-Instance Metrics.
- Search bar: Search for any metric, dimension or resource id.
- Table header:

	Instance Name (192)	InstanceId	Metric Name
--	---------------------	------------	-------------
- Table body:

<input type="checkbox"/>	my-instance	i-abbc12a7	CPUUtilization
<input type="checkbox"/>	my-instance		DiskReadBytes
<input type="checkbox"/>	my-instance		DiskReadOps
<input type="checkbox"/>	my-instance		DiskWriteBytes
<input type="checkbox"/>	my-instance		DiskWriteOps
<input type="checkbox"/>	my-instance		NetworkIn
<input type="checkbox"/>	my-instance		NetworkOut
<input type="checkbox"/>	my-instance	i-abbc12a7	NetworkPacketsIn
<input type="checkbox"/>	my-instance	i-abbc12a7	NetworkPacketsOut
- A context menu is open over the 'Metric Name' column for the first row, listing options: Add to search, Search for this only, Add to graph, Graph this metric only, Graph all search results, and Jump to resource.

Listar métricas usando o AWS CLI

Use o comando [list-metrics](#) para listar as métricas do CloudWatch para suas instâncias.

Para listar todas as métricas disponíveis para o Amazon EC2 (AWS CLI)

O exemplo a seguir especifica o namespace AWS/EC2 para visualizar todas as métricas para o Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

A seguir está um exemplo de saída:

```
{
  "Metrics": [
    {
      "Namespace": "AWS/EC2",
      "Dimensions": [
        {
          "Name": "InstanceId",
          "Value": "i-1234567890abcdef0"
        }
      ],
      "MetricName": "NetworkOut"
    },
    {
      "Namespace": "AWS/EC2",
      "Dimensions": [
        {
          "Name": "InstanceId",
          "Value": "i-1234567890abcdef0"
        }
      ],
      "MetricName": "CPUUtilization"
    },
    {
      "Namespace": "AWS/EC2",
      "Dimensions": [
        {
          "Name": "InstanceId",
          "Value": "i-1234567890abcdef0"
        }
      ],
      "MetricName": "NetworkIn"
    },
    ...
  ]
}
```

Para listar todas as métricas disponíveis para uma instância (AWS CLI)

O exemplo a seguir especifica o namespace AWS/EC2 e a dimensão `InstanceId` para visualizar os resultados somente para a instância especificada.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --dimensions
  Name=InstanceId,Value=i-1234567890abcdef0
```

Para listar uma métrica em todas as instâncias (AWS CLI)

O exemplo a seguir especifica o namespace AWS/EC2 e o nome de uma métrica para visualizar os resultados somente para a métrica especificada.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --metric-name CPUUtilization
```

Obter estatísticas para as métricas das instâncias

Você pode obter estatísticas para as métricas do CloudWatch para suas instâncias.

Tópicos

- [Visão geral das estatísticas \(p. 914\)](#)
- [Obter estatísticas para uma instância específica \(p. 914\)](#)
- [Aregar estatísticas entre instâncias \(p. 918\)](#)
- [Aregar estatísticas por grupo de Auto Scaling \(p. 920\)](#)
- [Aregar estatísticas por AMI \(p. 921\)](#)

Visão geral das estatísticas

Estatísticas são agregações de dados de métrica ao longo de períodos especificados. O CloudWatch fornece estatísticas com base nos pontos de dados de métrica fornecidos por seus dados personalizados ou por outros serviços na AWS para o CloudWatch. As agregações são feitas usando o namespace, o nome da métrica, as dimensões e a unidade de medida do ponto de dados no período especificado. A tabela a seguir descreve as estatísticas disponíveis.

Estatística	Descrição
Minimum	O valor mais baixo observado durante o período especificado. Você pode usar esse valor para determinar baixos volumes de atividade para a sua aplicação.
Maximum	O valor mais alto observado durante o período especificado. Você pode usar esse valor para determinar altos volumes de atividade para a sua aplicação.
Sum	Todos os valores enviados para a métrica correspondente, somados. Essa estatística pode ser útil para determinar o volume total de uma métrica.
Average	O valor de Sum / SampleCount durante o período especificado. Ao comparar essa estatística com o Minimum e o Maximum, você pode determinar o escopo completo de uma métrica e a proximidade da média de uso com o Minimum e o Maximum. Essa comparação ajuda você a saber quando aumentar ou diminuir seus recursos conforme necessário.
SampleCount	A contagem (número) de pontos de dados usados para o cálculo estatístico.
pNN.NN	O valor do percentil especificado. Você pode especificar qualquer percentil usando até duas casas decimais (por exemplo, p95.45).

Obter estatísticas para uma instância específica

Os exemplos a seguir mostram como usar o AWS Management Console ou a AWS CLI para determinar a utilização horária de CPU de uma instância do EC2 específica.

Requirements

- Você deve ter o ID da instância. É possível obter o ID da instância usando o AWS Management Console ou o comando [Describe-instances](#).

- Por padrão, o monitoramento básico é ativado, mas você pode habilitar o monitoramento detalhado. Para obter mais informações, consulte [Habilitar ou desabilitar o monitoramento detalhado para instâncias \(p. 899\)](#).

Para exibir a utilização de CPU para uma instância específica (console)

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace de métricas do EC2.

The screenshot shows the AWS CloudWatch Metrics console interface. At the top, there are three tabs: 'All metrics', 'Graphed metrics' (which is highlighted in orange), and 'Graph options'. Below the tabs is a search bar with the placeholder text 'Search for any metric, dimension or resource id'. The main area displays a grid of service names and their respective metric counts:

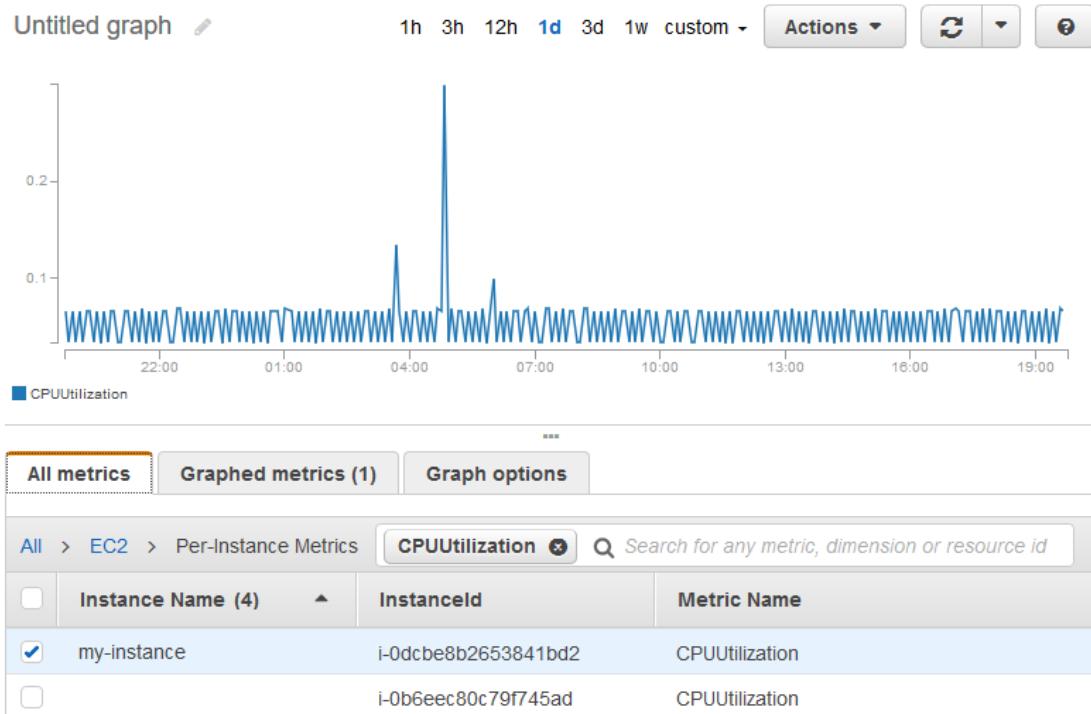
Service	Metrics
EBS	117 Metrics
EC2	316 Metrics
EFS	7 Metrics
ELB	210 Metrics
ElasticBeanstalk	8 Metrics
RDS	60 Metrics
S3	4 Metrics

4. Escolha a dimensão Per-Instance Metrics (Métricas por instância).

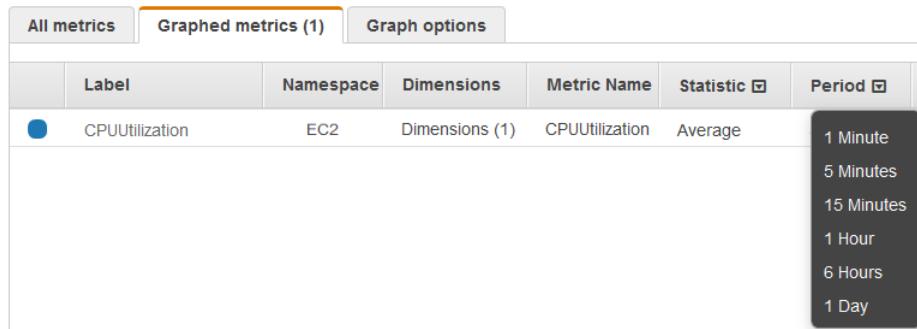
The screenshot shows the CloudWatch Metrics interface for EC2. At the top, there are three tabs: 'All metrics' (selected), 'Graphed metrics', and 'Graph options'. Below the tabs is a breadcrumb navigation bar: 'All > EC2'. To the right of the breadcrumb is a search bar with the placeholder 'Search for any metric, dimension or resource id'. The main content area displays '103 Metrics' and is organized into five categories:

- By Auto Scaling Group**: 28 Metrics
- By Image (AMI) Id**: 7 Metrics
- Per-Instance Metrics**: 54 Metrics
- Aggregated by Instance Type**: 7 Metrics
- Across All Instances**: 7 Metrics

5. No campo de pesquisa, digite **CPUutilization** e pressione Enter. Escolha a linha da instância específica, que exibe um gráfico da métrica CPUUtilization para a instância. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).



6. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.



Para obter a utilização de CPU para uma instância específica (AWS CLI)

Use o comando `get-metric-statistics` para obter a métrica CPUUtilization da instância específica usando o período e o intervalo de tempo especificados:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2016-10-18T23:18:00 --end-time 2016-10-19T23:18:00
```

A seguir está um exemplo de saída. Cada valor representa a porcentagem máxima de utilização da CPU para uma única instância do EC2.

```
{
  "Datapoints": [
```

```
{  
    "Timestamp": "2016-10-19T00:18:00Z",  
    "Maximum": 0.3300000000000002,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2016-10-19T03:18:00Z",  
    "Maximum": 99.67000000000002,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2016-10-19T07:18:00Z",  
    "Maximum": 0.3400000000000002,  
    "Unit": "Percent"  
},  
{  
    "Timestamp": "2016-10-19T12:18:00Z",  
    "Maximum": 0.3400000000000002,  
    "Unit": "Percent"  
},  
...  
],  
"Label": "CPUUtilization"  
}
```

Agregar estatísticas entre instâncias

Estatísticas agregadas estão disponíveis para as instâncias que têm o monitoramento detalhado habilitado. As instâncias que usam o monitoramento básico não estão incluídas nos agregados. Antes que seja possível obter estatísticas agregadas em todas as instâncias, você deve [habilitar o monitoramento detalhado \(p. 899\)](#) (a uma cobrança adicional), que fornece dados em períodos de um minuto.

O Amazon CloudWatch não pode agregar dados entre regiões da AWS. As métricas são completamente separadas entre regiões.

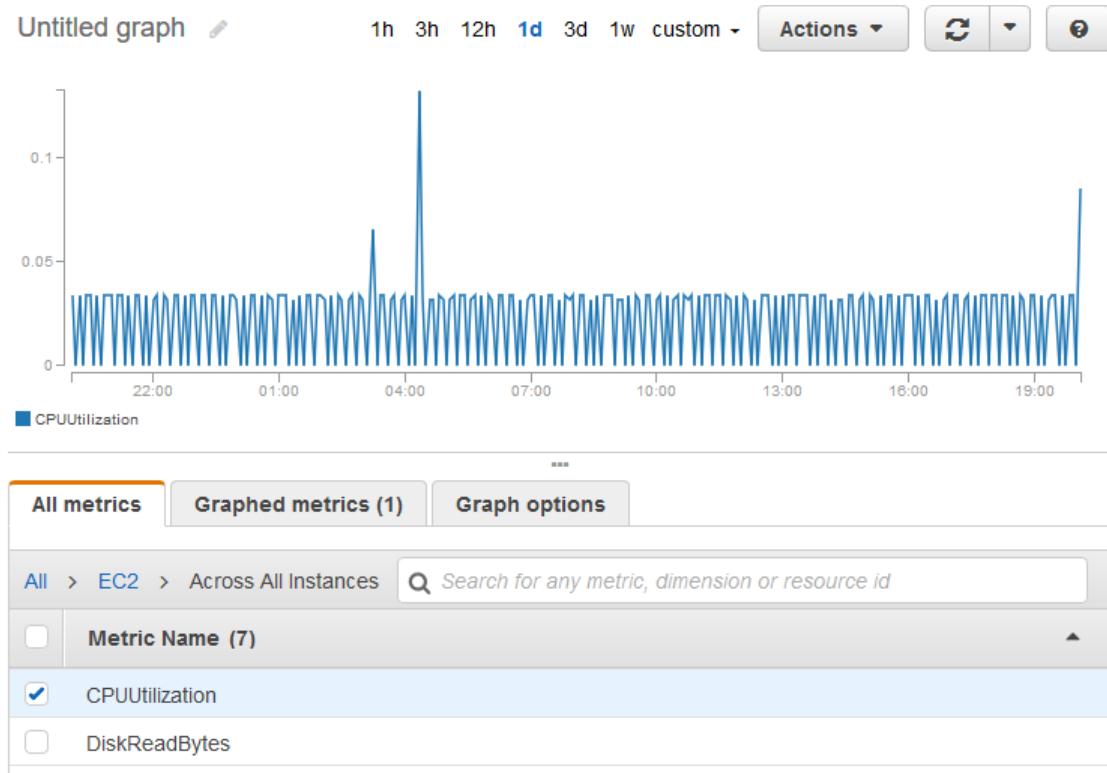
Este exemplo mostra a você como usar o monitoramento detalhado para obter uso médio de CPU para suas instâncias do EC2. Como nenhuma dimensão é especificada, o CloudWatch retorna estatísticas para todas as dimensões no namespace AWS/EC2.

Important

Essa técnica para recuperar todas as dimensões em um namespace da AWS não funciona para namespaces personalizados que você publicar no Amazon CloudWatch. Com namespaces personalizados, você deve especificar o conjunto completo de dimensões associadas a um determinado ponto de dados para recuperar estatísticas que incluem o ponto de dados.

Para exibir a utilização média de CPU em suas instâncias (console)

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace EC2 e escolha Across All Instances (Em todas as instâncias).
4. Escolha a linha que contém CPUUtilization, que exibe um gráfico da métrica para todas as instâncias do EC2. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).



5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para obter a utilização média de CPU em suas instâncias (AWS CLI)

Use o comando [get-metric-statistics](#) da seguinte forma para obter a média da métrica CPUUtilization em todas as suas instâncias.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/EC2 \
--metric-name CPUUtilization \
--period 3600 --statistics "Average" "SampleCount" \
--start-time 2016-10-11T23:18:00 \
--end-time 2016-10-12T23:18:00
```

A seguir está um exemplo de saída:

```
{
  "Datapoints": [
    {
      "SampleCount": 238.0,
      "Timestamp": "2016-10-12T07:18:00Z",
      "Average": 0.038235294117647062,
      "Unit": "Percent"
    },
    {
      "SampleCount": 240.0,
      "Timestamp": "2016-10-12T09:18:00Z",
      "Average": 0.16670833333333332,
      "Unit": "Percent"
    }
  ]
}
```

```
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2016-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Agregar estatísticas por grupo de Auto Scaling

Você pode agregar estatísticas para as instâncias do EC2 em um grupo do Auto Scaling. O Amazon CloudWatch não pode agregar dados entre regiões da AWS. As métricas são completamente separadas entre regiões.

Este exemplo mostra como recuperar o total de bytes gravados em disco para um grupo do Auto Scaling. O total é calculado para períodos de 1 minuto para um intervalo de 24 horas em todas as instâncias do EC2 no grupo do Auto Scaling especificado.

Para exibir DiskWriteBytes para as instâncias em um grupo do Auto Scaling (console)

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace EC2 e escolha By Auto Scaling Group (Por grupo de Auto Scaling).
4. Escolha a linha da métrica DiskWriteBytes e o grupo do Auto Scaling específico, que exibe um gráfico da métrica para as instâncias no grupo do Auto Scaling. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).
5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para exibir DiskWriteBytes para as instâncias em um grupo do Auto Scaling (AWS CLI)

Use o comando [get-metric-statistics](#) da seguinte forma.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes --
period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2016-10-16T23:18:00 --end-time 2016-10-18T23:18:00
```

A seguir está um exemplo de saída:

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2016-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2016-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        }
    ]
}
```

```
        "Unit": "Bytes"
    },
    "Label": "DiskWriteBytes"
}
```

Agregar estatísticas por AMI

Você pode agregar estatísticas para suas instâncias com monitoramento detalhado habilitado. As instâncias que usam o monitoramento básico não estão incluídas nos agregados. Antes que seja possível obter estatísticas agregadas em todas as instâncias, você deve [habilitar o monitoramento detalhado \(p. 899\)](#) (a uma cobrança adicional), que fornece dados em períodos de um minuto.

O Amazon CloudWatch não pode agregar dados entre regiões da AWS. As métricas são completamente separadas entre regiões.

Este exemplo mostra como determinar a utilização média da CPU para todas as instâncias que usam uma imagem de máquina da Amazon (AMI) específica. A média é intervalos de mais de 60 segundos para um período de um dia.

Para exibir a utilização média de CPU por AMI (console)

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Metrics (Métricas).
3. Escolha o namespace EC2 e escolha By Image (AMI) Id (Por ID de imagem (AMI)).
4. Escolha a linha da métrica CPUUtilization e a AMI específica, que exibe um gráfico da métrica para a AMI especificada. Para dar nome a um gráfico, selecione o ícone do lápis. Para alterar o período, selecione um dos valores predefinidos ou escolha custom (personalizado).
5. Para alterar a estatística ou o período da métrica, selecione a guia Graphed metrics (Métricas em gráfico). Escolha o cabeçalho de coluna ou um valor individual e, em seguida, escolha um valor diferente.

Para obter utilização média de CPU para um ID de imagem (AWS CLI)

Use o comando [get-metric-statistics](#) da seguinte forma.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --
period 3600 \
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2016-10-10T00:00:00 --end-time 2016-10-11T00:00:00
```

A seguir está um exemplo de saída. Cada valor representa uma porcentagem de utilização média da CPU para as instâncias do EC2 que executam a AMI especificada.

```
{
    "Datapoints": [
        {
            "Timestamp": "2016-10-10T07:00:00Z",
            "Average": 0.04100000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2016-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        }
    ]
}
```

```
        "Timestamp": "2016-10-10T06:00:00Z",
        "Average": 0.03600000000000011,
        "Unit": "Percent"
    },
    ...
],
"Label": "CPUUtilization"
}
```

Representar métricas em gráficos para as instâncias

Depois que executar uma instância, você pode abrir o console do Amazon EC2 e ver os gráficos de monitoramento para a instância na guia Monitoring (Monitoramento). Cada gráfico se baseia em uma das métricas disponíveis do Amazon EC2.

Os gráficos a seguir estão disponíveis:

- Utilização média da CPU (porcentagem)
- Leituras médias do disco (bytes)
- Gravações médias em disco (bytes)
- Rede máxima dentro (bytes)
- Rede máxima fora (bytes)
- Operações de leitura de disco de resumo (contagem)
- Operações de gravação de disco de resumo (contagem)
- Status de resumo (qualquer)
- Instância do status de resumo (contagem)
- Sistema de status de resumo (contagem)

Para mais informações sobre as métricas e os dados que elas fornecem aos gráficos, consulte [Listar as métricas disponíveis do CloudWatch para as instâncias \(p. 901\)](#).

Represente graficamente métricas usando o console CloudWatch

Você também pode usar o console do CloudWatch para representar graficamente os dados gerados pelo Amazon EC2 e outros produtos da AWS. Para obter mais informações, consulte [Represente métricas em gráficos](#) no Guia do usuário do Amazon CloudWatch.

Criar um alarme do CloudWatch para uma instância

Você pode criar um alarme do CloudWatch que monitore métricas do CloudWatch de uma de suas instâncias. O CloudWatch enviará automaticamente para você uma notificação quando a métrica atingir um limite especificado. Você pode criar um alarme do CloudWatch usando o console do Amazon EC2 ou usar as opções mais avançadas fornecidas pelo console do CloudWatch.

Para criar um alarme usando o console do CloudWatch

Para ver exemplos, consulte [Criação de alarmes do Amazon CloudWatch](#) no Guia do usuário do Amazon CloudWatch.

New console

Para criar um alarme usando o console do Amazon EC2

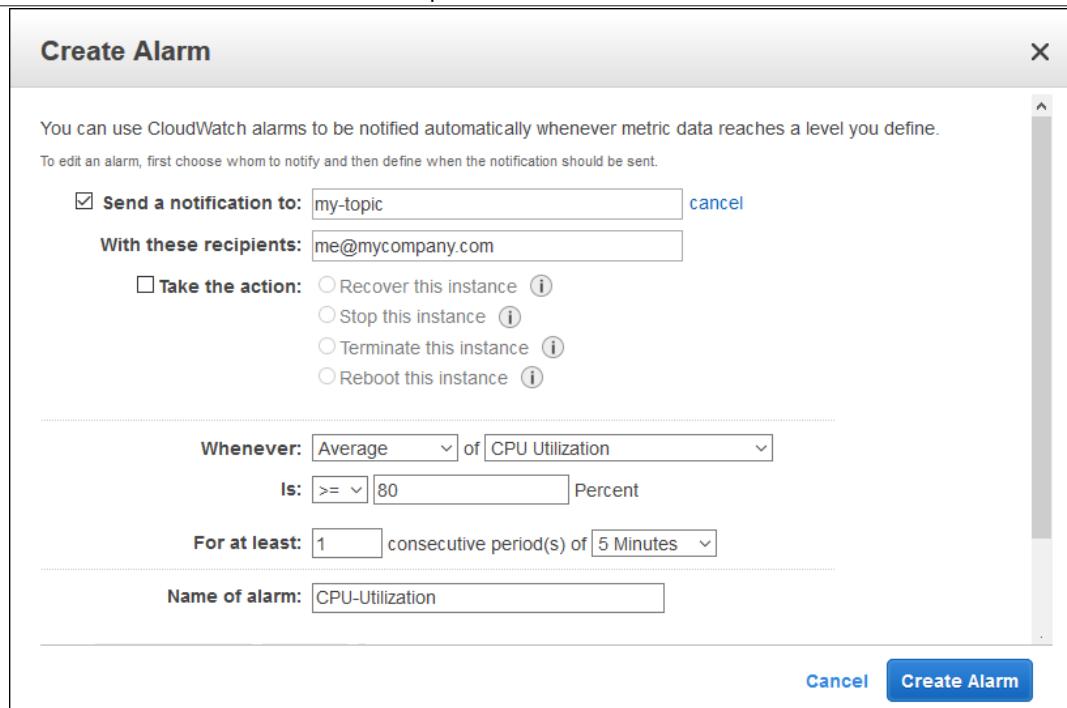
1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).
4. Na página de detalhes Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), em Add or edit alarm (Adicionar ou editar alarme), selecione Create an alarm (Criar alarme).
5. Em Alarm notification (Notificação de alarme), ative ou desative para configurar as notificações de Amazon Simple Notification Service (Amazon SNS). Insira um tópico de Amazon SNS existente ou insira um nome para criar um tópico.
6. Em Alarm action (Ação de alarme), selecione se deseja ativar ou desativar para especificar uma ação a ser executada quando o alarme for acionado. Selecione uma ação no menu suspenso.
7. Em Alarm thresholds (Limites de alarme), selecione a métrica e os critérios do alarme. Por exemplo, é possível sair das configurações padrão de Group samples by (Agrupar amostras por) (Average (Média)) e Type of data to sample (Tipo de dados para amostra) (CPU utilization (Uso da CPU)). Em Alarm when (Tocar alarme quando), escolha \geq e insira **0 . 80**. Em Consecutive period (Período consecutivo), insira **1**. Em Period (Período), selecione 5 minutes (5 minutos).
8. (Opcional) Em Sample metric data (Dados de métrica de exemplo), escolha Add to dashboard (Adicionar ao painel).
9. Escolha Create (Criar).

Old console

Para criar um alarme usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Monitoramento localizada na parte inferior da página, escolha Criar alarme. Ou, no menu suspenso Ações, escolha Monitoramento do CloudWatch, Adicionar/editar alarme.
5. Na caixa de diálogo Create Alarm (Criar alarme), faça o seguinte:
 - a. Escolha create topic (criar tópico). Em Send a notification to (Enviar uma notificação para), digite um nome do tópico do SNS. Em With these recipients (Com estes destinatários), digite um ou mais endereços de email para receber a notificação.
 - b. Especifique a métrica e os critérios da política. Por exemplo, você pode deixar as configurações padrão para Whenever (Sempre) (média de utilização de CPU). Em Is (É), escolha \geq e digite 80 por cento. Em For at least (Para pelo menos), digite 1 período consecutivo de 5 Minutes.
 - c. Escolha Create Alarm.



Você pode editar suas configurações de alarme do CloudWatch no console do Amazon EC2 ou no console do CloudWatch. Se você quiser excluir seu alarme, poderá fazê-lo a partir no console do CloudWatch. Para obter mais informações, consulte [Editar ou excluir um alarme do CloudWatch](#) no Guia do usuário do Amazon CloudWatch.

Criar alarmes para interromper, encerrar, reiniciar ou recuperar uma instância

Usando as ações de alarme do Amazon CloudWatch, você cria alarmes que automaticamente param, encerram, reinicializam ou recuperam suas instâncias. Você pode usar as ações de parada ou encerramento para ajudar a economizar dinheiro quando não precisar mais que uma instância seja executada. Você pode usar as ações de reinicialização e recuperação para reiniciar automaticamente essas instâncias ou recuperá-las para um novo hardware caso ocorra um problema no sistema.

A função `AWSLambdaRoleForCloudWatchEvents` ligado ao serviço permite que a AWS execute ações de alarme em seu nome. A primeira vez que criar um alarme no AWS Management Console, na CLI do IAM ou na API do IAM, o CloudWatch cria a função vinculada ao serviço para você.

Há várias situações nas quais você pode querer interromper ou encerrar sua instância automaticamente. Por exemplo, você pode ter instâncias dedicadas a trabalhos de processamento de folha de pagamento em lote ou tarefas de computação científica que são executadas por um período e, em seguida, concluem seu trabalho. Em vez de permitir que essas instâncias fiquem ociosas (e acumulem cobranças), você pode interrompê-las ou encerrá-las, o que pode ajudá-lo a fazer uma economia. A principal diferença entre usar as ações de alarme de interrupção e encerramento é que é possível facilmente iniciar uma instância interrompida se precisar executá-la novamente mais tarde e manter o mesmo ID de instância e volume do dispositivo raiz. No entanto, não é possível iniciar uma instância encerrada. Em vez disso, você deve executar uma nova instância.

É possível adicionar as ações de interrupção, encerramento, reinicialização ou recuperação a qualquer alarme definido em uma métrica por instância do Amazon EC2, incluindo métricas de monitoramento básico e detalhado fornecidas pelo Amazon CloudWatch (no namespace AWS/EC2), bem como todas as métricas personalizadas que incluem a dimensão InstanceId, desde que seu valor se refira a uma instância do Amazon EC2 em execução.

Supporte a consoles

Você pode criar alarmes usando o console do Amazon EC2 ou do CloudWatch. Os procedimentos nesta documentação usam o console do Amazon EC2. Para procedimentos que usam o console do CloudWatch, consulte [Criar alarmes que param, encerram, reinicializam ou recuperam uma instância](#) no Guia do usuário do Amazon CloudWatch.

Permissions

Se você é um usuário do AWS Identity and Access Management (IAM), deve ter o `iam:CreateServiceLinkedRole` para criar ou modificar um alarme que executa ações de alarme EC2.

Tópicos

- [Adicionar ações de interrupção a alarmes do Amazon CloudWatch \(p. 925\)](#)
- [Adicionar ações de encerramento a alarmes do Amazon CloudWatch \(p. 927\)](#)
- [Adicionar ações de reinicialização a alarmes do Amazon CloudWatch \(p. 928\)](#)
- [Adicionar ações de recuperação a alarmes do Amazon CloudWatch \(p. 930\)](#)
- [Usar o console do Amazon CloudWatch para visualizar o histórico do alarme e da ação \(p. 932\)](#)
- [Cenários de ação do alarme do Amazon CloudWatch \(p. 933\)](#)

Adicionar ações de interrupção a alarmes do Amazon CloudWatch

Você pode criar um alarme que pare uma instância do Amazon EC2 quando o limite for atingido. Por exemplo, você pode executar instâncias de desenvolvimento ou teste e ocasionalmente se esquecer de desativá-las. Você pode criar um alarme que seja acionado quando o percentual médio de utilização da CPU for inferior a 10% em 24 horas, sinalizando que ela está ociosa e não mais em uso. Você pode ajustar o limite, a duração e o período para atender às suas necessidades, além de poder adicionar uma notificação do Amazon Simple Notification Service (Amazon SNS) para receber um e-mail quando o alarme for acionado.

As instâncias que usam um volume do Amazon EBS como dispositivo raiz podem ser interrompidas ou encerradas, enquanto as instâncias que usam o armazenamento de instância como dispositivo raiz só podem ser encerradas.

New console

Para criar um alarme para parar uma instância em repouso (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

Como alternativa, você pode escolher o sinal de mais (+) na coluna Alarm status (Status do alarme).

4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:

- a. Escolha Create an alarm (Criar um alarme).
- b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte [Usar o Amazon SNS para mensagens de aplicativo para pessoa \(A2P\)](#) no Guia do desenvolvedor do Amazon Simple Notification Service.
- c. Alterne em Alarm action (Ação alarme) para Stop (Parar).
- d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e CPU utilization (Utilização da CPU).
- e. Para Alarm When (Alarme quando) e Percent (Percentual), especifique o limite da métrica. Neste exemplo, especifique <= e 10%.
- f. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, especifique 1 período consecutivo de 5 minutos.
- g. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

Note

Você pode ajustar a configuração do alarme com base em suas próprias necessidades antes de criá-lo, ou pode editá-las mais tarde. Aí incluem-se as configurações de métrica, limiar, duração, ação e notificação. No entanto, depois de criar um alarme, você não pode mais editar seu nome.

- h. Escolha Create (Criar).

Old console

Para criar um alarme para parar uma instância em repouso (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância. Na guia Monitoramento, selecione Criar alarme.
4. Na caixa de diálogo Create Alarm (Criar alarme), faça o seguinte:
 - a. Para receber um e-mail quando o alarme for acionado, na caixa de diálogo Send a notification to (Enviar uma notificação para), escolha um tópico existente do Amazon SNS ou selecione Create topic (Criar tópico) para criar um tópico novo.

Para criar um novo tópico, em Send a notification to (Enviar notificação para), digite um nome para o tópico e, em seguida, em With these recipients (Com estes destinatários), digite os endereços de e-mail dos destinatários (separados por vírgulas). Depois de criar o alarme, você receberá um e-mail de confirmação da inscrição que você deve aceitar antes de receber notificações para este tópico.
 - b. Escolha Take the action (Executar a ação), escolha Stop this instance (Interromper a instância).
 - c. Para Sempre, selecione a estatística que você deseja usar e escolha a métrica. Neste exemplo, escolha Média e Utilização da CPU.
 - d. Para Is, especifique o limite da métrica. Neste exemplo, digite 10 por cento.
 - e. Em For at least (Durante pelo menos), especifique o período de avaliação do alarme. Neste exemplo, digite 24 períodos consecutivos de 1 hora.
 - f. Para alterar o nome do alarme, em Name of alarm (Nome do alarme), digite um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

Se você não digitar um nome para o alarme, o Amazon CloudWatch criará um automaticamente.

Note

Você pode ajustar a configuração do alarme com base em suas próprias necessidades antes de criá-lo, ou pode editá-las mais tarde. Aí incluem-se as configurações de métrica, limiar, duração, ação e notificação. No entanto, depois de criar um alarme, você não pode mais editar seu nome.

- g. Escolha Create Alarm.

Adicionar ações de encerramento a alarmes do Amazon CloudWatch

Você pode criar um alarme que encerre uma instância do EC2 automaticamente quando um certo limite for atingido (desde que a proteção contra encerramento não esteja ativada para a instância). Por exemplo, você pode encerrar uma instância quando ela tiver concluído seu trabalho e não precisar mais dela. Se você quiser usar a instância posteriormente, pare-a em vez de encerrá-la. Para obter informações sobre como habilitar e desabilitar a proteção contra encerramento de uma instância, consulte [Habilitar a proteção contra encerramento \(p. 476\)](#).

New console

Para criar um alarme para encerrar uma instância em repouso (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

Como alternativa, você pode escolher o sinal de mais () na coluna Alarm status (Status do alarme) .

4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:
 - a. Escolha Create an alarm (Criar um alarme).
 - b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte [Usar o Amazon SNS para mensagens de aplicativo para pessoa \(A2P\)](#) no Guia do desenvolvedor do Amazon Simple Notification Service.
 - c. Alterne em Alarm action (Ação alarme)e escolha Terminate (Encerrar).
 - d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e CPU utilization (Utilização da CPU).
 - e. Para Alarm When (Alarme quando) e Percent (Percentual), especifique o limite da métrica. Neste exemplo, especifique => e 10 por cento.
 - f. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, especifique 24 períodos consecutivos de 1 hora.
 - g. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

Note

Você pode ajustar a configuração do alarme com base em suas próprias necessidades antes de criá-lo, ou pode editá-las mais tarde. Aí incluem-se as configurações de métrica, limiar, duração, ação e notificação. No entanto, depois de criar um alarme, você não pode mais editar seu nome.

- h. Escolha Create (Criar).

Old console

Para criar um alarme para encerrar uma instância em repouso (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância. Na guia Monitoramento, selecione Criar alarme.
4. Na caixa de diálogo Create Alarm (Criar alarme), faça o seguinte:
 - a. Para receber um e-mail quando o alarme for acionado, na caixa de diálogo Send a notification to (Enviar uma notificação para), escolha um tópico existente do Amazon SNS ou selecione Create topic (Criar tópico) para criar um tópico novo.
Para criar um novo tópico, em Send a notification to (Enviar notificação para), digite um nome para o tópico e, em seguida, em With these recipients (Com estes destinatários), digite os endereços de e-mail dos destinatários (separados por vírgulas). Depois de criar o alarme, você receberá um e-mail de confirmação da inscrição que você deve aceitar antes de receber notificações para este tópico.
 - b. Escolha Take the action (Executar a ação), escolha Terminate this instance (Encerrar a instância).
 - c. Para Sempre, escolha uma estatística e, então, a métrica. Neste exemplo, escolha Média e Utilização da CPU.
 - d. Para Is, especifique o limite da métrica. Neste exemplo, digite 10 por cento.
 - e. Em For at least (Durante pelo menos), especifique o período de avaliação do alarme. Neste exemplo, digite 24 períodos consecutivos de 1 hora.
 - f. Para alterar o nome do alarme, em Name of alarm (Nome do alarme), digite um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

Se você não digitar um nome para o alarme, o Amazon CloudWatch criará um automaticamente.

Note

Você pode ajustar a configuração do alarme com base em suas próprias necessidades antes de criá-lo, ou pode editá-las mais tarde. Aí incluem-se as configurações de métrica, limiar, duração, ação e notificação. No entanto, depois de criar um alarme, você não pode mais editar seu nome.

- g. Escolha Create Alarm.

Adicionar ações de reinicialização a alarmes do Amazon CloudWatch

Você pode criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2 e reinicie automaticamente a instância. A ação de alarme de reinicialização é recomendada para falhas de verificação de integridade da instância (ao contrário da ação de alarme de recuperação, que

é adequado para falhas de verificação de integridade do sistema). Reiniciar a instância equivale a reiniciar o sistema operacional. Na maioria dos casos, leva apenas alguns minutos para reiniciar sua instância. Quando você reinicia uma instância, ela permanece no mesmo host físico, para que sua instância mantenha seu nome DNS público, o endereço IP privado e os dados em seus volumes de armazenamento de instância.

A reinicialização de uma instância não inicia uma nova hora de faturamento de instância (com uma cobrança mínima de um minuto), diferente do que acontece na interrupção e na reinicialização da instância. Para obter mais informações, consulte [Reiniciar a instância \(p. 470\)](#).

Important

Para evitar um comportamento de disputa entre as ações de reinicialização e recuperação, evite configurar o mesmo número de períodos de avaliação para um alarme de reinicialização e um alarme de recuperação. Recomendamos que você defina alarmes de reinicialização para três períodos de avaliação de um minuto cada. Para obter mais informações, consulte [Avaliar um alarme no Guia do usuário do Amazon CloudWatch](#).

New console

Para criar um alarme para reiniciar uma instância (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

Como alternativa, você pode escolher o sinal de mais (+) na coluna Alarm status (Status do alarme).

4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:
 - a. Escolha Create an alarm (Criar um alarme).
 - b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte [Usar o Amazon SNS para mensagens de aplicativo para pessoa \(A2P\)](#) no Guia do desenvolvedor do Amazon Simple Notification Service.
 - c. Alterne em Alarm action (Ação alarme) e escolha Reboot (Reiniciar).
 - d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e Status check failed: instance (Falha na verificação de status: instância).
 - e. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, digite 3 períodos consecutivos de 5 minutos.
 - f. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.
 - g. Escolha Create (Criar).

Old console

Para criar um alarme para reiniciar uma instância (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).

3. Selecione a instância. Na guia Monitoramento, selecione Criar alarme.

4. Na caixa de diálogo Create Alarm (Criar alarme), faça o seguinte:

- a. Para receber um e-mail quando o alarme for acionado, na caixa de diálogo Send a notification to (Enviar uma notificação para), escolha um tópico existente do Amazon SNS ou selecione Create topic (Criar tópico) para criar um tópico novo.

Para criar um novo tópico, em Send a notification to (Enviar notificação para), digite um nome para o tópico e, em With these recipients (Com estes destinatários), digite os endereços de e-mail dos destinatários (separados por vírgulas). Depois de criar o alarme, você receberá um e-mail de confirmação da inscrição que você deve aceitar antes de receber notificações para este tópico.

- b. Selecione Take the action (Executar a ação), escolha Reboot this instance (Reiniciar a instância).
- c. Para Sempre, escolha Falha na verificação de status (instância).
- d. Em For at least (Durante pelo menos), especifique o período de avaliação do alarme. Neste exemplo, digite 3 períodos consecutivos de 5 minutos.
- e. Para alterar o nome do alarme, em Name of alarm (Nome do alarme), digite um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

Se você não digitar um nome para o alarme, o Amazon CloudWatch criará um automaticamente.

- f. Escolha Create Alarm.

Adicionar ações de recuperação a alarmes do Amazon CloudWatch

Você pode criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2. Se a instância for invalidada devido a uma falha de hardware subjacente ou a um problema que exija o envolvimento da AWS para corrigi-lo, você poderá recuperar a instância automaticamente. Instâncias encerradas não podem ser recuperadas. Uma instância recuperada é idêntica à instância original, incluindo o ID da instância, endereços IP privados, endereços IP elásticos e todos os metadados de instância.

O CloudWatch impede que você adicione uma ação de recuperação a um alarme que esteja em uma instância que não oferece suporte a ações de recuperação.

Quando o alarme `StatusCheckFailed_System` for acionado e a ação de recuperação for iniciada, você será notificado pelo tópico do Amazon SNS que escolheu ao criar o alarme e a ação de recuperação associada. Durante a recuperação da instância, a instância será migrada durante uma reinicialização da instância e todos os dados na memória serão perdidos. Quando o processo é concluído, as informações serão publicadas no tópico do SNS que você tiver configurado para o alarme. Qualquer pessoa que estiver inscrita neste tópico do SNS receberá uma notificação por e-mail com o status da tentativa de recuperação e instruções adicionais. Você perceberá uma reinicialização de instância na instância recuperada.

A ação de recuperação pode ser usada somente com `StatusCheckFailed_System`, não com `StatusCheckFailed_Instance`.

Os problemas a seguir podem causar falha nas verificações de status do sistema:

- Perda de conectividade de rede
- Perda de energia do sistema
- Problemas de software no host físico
- Problemas de hardware de host físico que afetam a acessibilidade de rede

A ação de recuperação é compatível somente nas instâncias com as seguintes características:

- Use um dos seguintes tipos de instância: C3, C4, C5, C5a, C5n, M3, M4, M5, M5a, M5n, M5zn, M6i, P3, R3, R4, R5, R5a, R5b, R5n, T2, T3, T3a, alta memória (apenas virtualizada), X1, X1e
- Use uma locação de instância **default** ou **dedicated**
- Use somente volumes do EBS (não configure volumes de armazenamento de instâncias). Para obter mais informações, consulte "[Recuperar esta instância](#)" está desabilitado.

Se a sua instância tiver um endereço IP público, ela reterá o endereço IP público após a recuperação.

Important

Para evitar um comportamento de disputa entre as ações de reinicialização e recuperação, evite configurar o mesmo número de períodos de avaliação para um alarme de reinicialização e um alarme de recuperação. É recomendável que você defina os alarmes de recuperação para dois períodos de avaliação de um minuto cada. Para obter mais informações, consulte [Como avaliar um alarme](#) em Guia do usuário do Amazon CloudWatch.

New console

Para criar um alarme para recuperar uma instância (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch).

Como alternativa, você pode escolher o sinal de mais (+) na coluna Alarm status (Status do alarme).

4. Na página Manage CloudWatch alarms (Gerenciar alarmes do CloudWatch), faça o seguinte:
 - a. Escolha Create an alarm (Criar um alarme).
 - b. Para receber um e-mail quando o alarme for acionado, para Alarm notification (Notificação de alarme), escolha um Amazon SNS tópico existente. Para fazer isso, você precisa criar um tópico do Amazon SNS usando o console do Amazon SNS. Para obter mais informações, consulte [Usar o Amazon SNS para mensagens de aplicativo para pessoa \(A2P\)](#) no Guia do desenvolvedor do Amazon Simple Notification Service.

Note

Os usuários devem se inscrever no tópico do SNS especificado para receber notificações por email quando o alarme for acionado. O usuário raiz da conta da AWS sempre recebe notificações por e-mail quando ocorrem ações de recuperação automática da instância, mesmo que um tópico do SNS não esteja especificado ou o usuário raiz não esteja inscrito no tópico do SNS especificado.

- c. Alterne em Alarm action (Ação alarme) e escolha Recover (Recuperar).
- d. Para Group samples by (Agrupar amostras por) e Type of data to sample (Tipo de dados a serem amostrados), escolha uma estatística e uma métrica. Neste exemplo, escolha Average (Média) e Status check failed: system (Falha na verificação de status: sistema).
- e. Para Consecutive period (Período consecutivo) e Period (Período), especifique o período de avaliação do alarme. Neste exemplo, digite 2 períodos consecutivos de 5 minutos.
- f. Amazon CloudWatch cria automaticamente um nome de alarme para você. Para alterar o nome, em Alarm name (Nome do alarme), insira um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

- g. Escolha Create (Criar).

Old console

Para criar um alarme para recuperar uma instância (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância. Na guia Monitoramento, selecione Criar alarme.
4. Na caixa de diálogo Create Alarm (Criar alarme), faça o seguinte:
 - a. Para receber um e-mail quando o alarme for acionado, na caixa de diálogo Send a notification to (Enviar uma notificação para), escolha um tópico existente do Amazon SNS ou selecione Create topic (Criar tópico) para criar um tópico novo.

Para criar um novo tópico, em Send a notification to (Enviar notificação para), digite um nome para o tópico e, em With these recipients (Com estes destinatários), digite os endereços de e-mail dos destinatários (separados por vírgulas). Depois de criar o alarme, você receberá um e-mail de confirmação da inscrição que você deve aceitar antes de receber e-mail para este tópico.

Note

- Os usuários devem se inscrever no tópico do SNS especificado para receber notificações por email quando o alarme for acionado.
- O usuário raiz da conta da AWS sempre recebe notificações por email quando ocorrem ações de recuperação automática da instância, mesmo que o tópico do SNS não seja especificado.
- O usuário raiz da conta da AWS sempre recebe notificações por email quando ocorrem ações de recuperação automática da instância, mesmo que não esteja inscrito no tópico do SNS especificado.

- b. Selecione Take the action (Executar a ação), escolha Recover this instance (Recuperar a instância).
- c. Para Sempre, escolha Falha na verificação de status (sistema).
- d. Em For at least (Durante pelo menos), especifique o período de avaliação do alarme. Neste exemplo, digite 2 períodos consecutivos de 5 minutos.
- e. Para alterar o nome do alarme, em Name of alarm (Nome do alarme), digite um novo nome. Os nomes de alarme devem conter somente caracteres ASCII.

Se você não digitar um nome para o alarme, o Amazon CloudWatch criará um automaticamente.

- f. Escolha Create Alarm.

Usar o console do Amazon CloudWatch para visualizar o histórico do alarme e da ação

É possível exibir o histórico de alarmes e ações no console do Amazon CloudWatch. O Amazon CloudWatch mantém as últimas duas semanas de histórico de alarmes e ações.

Para visualizar o histórico de alarmes e ações acionados (console do CloudWatch)

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Alarms.

-
3. Selecione um alarme.
 4. A guia Detalhes mostra a transição de estado mais recente juntamente com os valores de tempo e métrica.
 5. Escolha a guia Histórico para visualizar as entradas mais recentes do histórico.

Cenários de ação do alarme do Amazon CloudWatch

Você pode usar o console do Amazon EC2 para criar as ações de alarme que interrompem ou encerram uma instância do Amazon EC2 quando determinadas circunstâncias são atendidas. Na captura de tela a seguir da página do console onde você define as ações de alarme, nós numeramos as configurações. Nós também numeramos as configurações nos cenários a seguir, para ajudá-lo a criar as ações apropriadas.

New console

Alarm notification Info

Configure the alarm to send notifications to an Amazon SNS topic when it is triggered.

Choose an existing topic or enter a name to create a new topic

1

Alarm action Info

Specify the action to take when the alarm is triggered.

Selection action to alarm fires

Alarm thresholds

Specify the metric thresholds for the alarm.

Group samples by **2**: Page

Type of data to sample **3**:

Alarm When **4**:

Consecutive Period **5**:

Period **6**:

Alarm name **7**: awsec2-i-04a2b95d0495ac1ee-GreaterThanOrEqualToThreshold-

Old console

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.
To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: [create topic](#)

Take the action: Recover this instance [i](#)
 Stop this instance [i](#)
 Terminate this instance [i](#)
 Reboot this instance [i](#)

Whenever: of
Is: Percent

For at least: consecutive period(s) of

Name of alarm:

CPU Utilization Percent

75
50
25
0

7/21 7/22 7/22
22:00 00:00 02:00

[Cancel](#) [Create Alarm](#)

Cenário 1: interromper instâncias de teste e desenvolvimento ociosas

Crie um alarme que interrompa uma instância usada para desenvolvimento ou teste de software quando estiver inativa pelo menos uma hora.

Configuração	Valor
1	Interromper
2	Máximo
3	Utilização da CPU
4	<=
5	10%
6	1
7	1 hora

Cenário 2: interromper instâncias ociosas

Crie um alarme que interrompa uma instância e envie um e-mail quando a instância estiver inativa por 24 horas.

Configuração	Valor
1	Interromper e enviar e-mail
2	Média
3	Utilização da CPU
4	<=

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Criar alarmes para interromper, encerrar,
reiniciar ou recuperar uma instância

Configuração	Valor
5	5%
6	24
7	1 hora

Cenário 3: enviar e-mail em servidores Web com tráfego incomumente alto

Crie um alarme que envie o e-mail quando uma instância ultrapassar 10 GB de tráfego de rede de saída por dia.

Configuração	Valor
1	E-mail
2	Soma
3	Saída de rede
4	>
5	10 GB
6	24
7	1 hora

Cenário 4: interromper servidores Web com tráfego incomumente alto

Crie um alarme que pare uma instância e envie uma mensagem de texto (SMS) se o tráfego de saída exceder 1 GB por hora.

Configuração	Valor
1	Parar e enviar SMS
2	Soma
3	Saída de rede
4	>
5	1 GB
6	1
7	1 hora

Cenário 5: Interromper uma instância danificada

Crie um alarme que interrompa uma instância em falhe três verificações de status consecutivas (executadas em intervalos de 5 minutos).

Configuração	Valor
1	Interromper
2	Média
3	Falha na verificação de status: sistema
4	-
5	-
6	1
7	15 minutos

Cenário 6: Encerrar instâncias quando os trabalhos de processamento em lote estiverem concluídos

Crie um alarme que encerre uma instância que execute trabalhos em lote quando não estiver mais enviando os dados dos resultados.

Configuração	Valor
1	Encerrar
2	Máximo
3	Saída de rede
4	<=
5	100,000 bytes
6	1
7	5 minutos

Automatizar o Amazon EC2 com o EventBridge

O Amazon EventBridge permite que você automatize seus produtos da AWS e responda automaticamente aos eventos do sistema, como problemas de disponibilidade da aplicação ou alterações de recursos. Os eventos dos produtos da AWS são entregues ao EventBridge quase em tempo real. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. As ações que podem ser automaticamente acionadas incluem as seguintes:

- Como invocar uma função do AWS Lambda
- Invocação do Run Command do Amazon EC2
- Retransmissão do evento para o Amazon Kinesis Data Streams
- Ativação da máquina de estado do AWS Step Functions
- Notificação de um tópico do Amazon SNS ou de uma fila do Amazon SQS

Alguns exemplos de uso do EventBridge com o Amazon EC2 incluem:

- Ativação da função do Lambda sempre que um nova instância do Amazon EC2 é iniciada.
- Notificação de um tópico do Amazon SNS quando o volume do Amazon EBS é criado ou modificado.
- Envio de um comando para uma ou mais instâncias do Amazon EC2 usando o Run Command do Amazon EC2 sempre que determinado evento ocorre em outro produto da AWS.

Para obter mais informações, consulte o [Guia do usuário do Amazon EventBridge](#).

Registrar em log o Amazon EC2 e chamadas de APIs do Amazon EBS com o AWS CloudTrail

O Amazon EC2 e o Amazon EBS são integrados ao AWS CloudTrail, um serviço que fornece um registro de ações executadas por um usuário, uma função ou um produto da AWS no Amazon EC2 e Amazon EBS. O CloudTrail captura todas as chamadas de API para o Amazon EC2 e Amazon EBS como eventos, incluindo chamadas do console e de chamadas de código para as APIs. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos do Amazon EC2 e do Amazon EBS. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Com as informações coletadas pelo CloudTrail, você pode determinar a solicitação feita ao Amazon EC2 e ao Amazon EBS, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre o CloudTrail, consulte o [AWS CloudTrail User Guide](#) (Manual do usuário do AWS CloudTrail).

Informações sobre o Amazon EC2 e o Amazon EBS no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade no Amazon EC2 e no Amazon EBS, ela é registrada em um evento do CloudTrail com outros eventos de produtos da AWS no Event history (Histórico de eventos). Você pode visualizar, pesquisar e fazer download de eventos recentes em sua conta da AWS. Para obter mais informações, consulte [Como visualizar eventos com o histórico de eventos do CloudTrail](#).

Para obter um registro contínuo de eventos em sua conta da AWS, incluindo eventos do Amazon EC2 e do Amazon EBS, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da . A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, você pode configurar outros produtos da AWS para analisar mais profundamente e agir sobre os dados de eventos coletados nos logs do CloudTrail.

Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços e integrações compatíveis com o CloudTrail](#)
- [Configuração de notificações do Amazon SNS para o CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas](#)

Todas as ações do Amazon EC2 e as ações de gerenciamento do Amazon EBS são registradas pelo CloudTrail e documentadas na [Amazon EC2 API Reference](#) (Referência da API do Amazon EC2). Por exemplo, as chamadas às ações `RunInstances`, `DescribeInstances` ou `CreateImage` geram entradas nos arquivos de log do CloudTrail.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o [Elemento userIdentity do CloudTrail](#).

Noções básicas sobre entradas dos arquivos de log no Amazon EC2 e no Amazon EBS.

Uma trilha é uma configuração que permite a entrega de eventos como registros de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada das chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O arquivo de log a seguir mostra que um usuário encerrou uma instância.

```
{  
  "Records": [  
    {  
      "eventVersion": "1.03",  
      "userIdentity": {  
        "type": "Root",  
        "principalId": "123456789012",  
        "arn": "arn:aws:iam::123456789012:root",  
        "accountId": "123456789012",  
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
        "userName": "user"  
      },  
      "eventTime": "2016-05-20T08:27:45Z",  
      "eventSource": "ec2.amazonaws.com",  
      "eventName": "TerminateInstances",  
      "awsRegion": "us-west-2",  
      "sourceIPAddress": "198.51.100.1",  
      "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",  
      "requestParameters": {  
        "instancesSet": {  
          "items": [{  
            "instanceId": "i-1a2b3c4d"  
          }]  
        }  
      },  
      "responseElements": {  
        "instancesSet": {  
          "items": [{  
            "instanceId": "i-1a2b3c4d",  
            "currentState": {  
              "code": 32,  
              "name": "shutting-down"  
            },  
            "previousState": {  
              "code": 16,  
              "name": "running"  
            }  
          }]  
        }  
      }  
    }  
  ]  
}
```

```
        }]
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
]
```

Usar o AWS CloudTrail para auditar usuários que se conectam por EC2 Instance Connect

Use o AWS CloudTrail para auditar os usuários que se conectam às suas instâncias por meio do via EC2 Instance Connect.

Para auditar a atividade do SSH por meio do EC2 Instance Connect usando o console do AWS CloudTrail

1. Abra o console do AWS CloudTrail em <https://console.aws.amazon.com/cloudtrail/>.
2. Verifique se você está na região correta.
3. No painel de navegação, selecione Event history (Histórico de eventos).
4. Para Filter (Filtro), selecione Event source (Fonte do evento), ec2-instance-connect.amazonaws.com.
5. (Opcional) Para Time range (Intervalo de tempo), selecione um intervalo de tempo.
6. Selecione o ícone Refresh events (Atualizar eventos).
7. A página exibe os eventos que correspondem às chamadas da API [SendsShPublicKey](#). Expanda um evento usando a seta para exibir detalhes adicionais, como nome de usuário e chave de acesso da AWS usada para fazer a conexão SSH e o endereço IP de origem.
8. Para exibir todas as informações do evento no formato JSON, selecione View event (Exibir evento). O campo requestParameters contém o ID da instância de destino, o nome do usuário do sistema operacional e a chave pública usada para fazer a conexão do SSH.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGHIJKLMNO9876543210EXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"
            }
        },
        "eventTime": "2018-09-21T21:38:00Z",
        "eventSource": "ec2-instance-connect.amazonaws.com",
        "eventName": "SendSSHPublicKey",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "123.456.789.012",
        "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
        "requestParameters": {
            "instanceId": "i-0123456789EXAMPLE",
            "osUser": "ec2-user",
        }
    }
}
```

```
"SSHKey": {  
    "publicKey": "ssh-rsa ABCDEFGHIJKLMNOP01234567890EXAMPLE"  
}  
},  
"responseElements": null,  
"requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",  
"eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",  
"eventType": "AwsApiCall",  
"recipientAccountId": "0987654321"  
}
```

Se você tiver configurado a conta da AWS para coletar eventos do CloudTrail em um bucket do S3, poderá fazer download e auditar as informações de forma programática. Para obter mais informações, consulte [Getting and Viewing Your CloudTrail Log Files](#) (Obter e visualizar seus arquivos de log do CloudTrail) no AWS CloudTrail User Guide (Manual do usuário do AWS CloudTrail).

Monitorar as aplicações .NET e SQL Server com o CloudWatch Application Insights

O CloudWatch Application Insights for .NET e SQL Server ajuda você a monitorar as aplicações .NET e SQL Server que usam instâncias do Amazon EC2 juntamente com outros [recursos de aplicações da AWS](#). Ele identifica e configura os principais logs de métricas e alarmes na pilha de tecnologia e nos recursos da aplicação (por exemplo, banco de dados Microsoft SQL Server, servidores Web (IIS) e de aplicações, SO, load balancers e filas). Ele monitora continuamente os logs e as métricas para detectar e correlacionar anomalias e erros. Quando erros e anomalias são detectados, o Application Insights gera o [CloudWatch Events](#) que você pode usar para configurar notificações ou executar ações. Para auxiliar na solução de problemas, ele cria painéis automatizados para os problemas detectados, que incluem anomalias de métricas correlacionadas e erros de log com informações adicionais para indicar a potencial causa do problema. Os painéis automatizados ajudam você a tomar medidas corretivas rápidas para manter suas aplicações íntegras e para evitar o impacto nos usuários finais da sua aplicação.

Para visualizar uma lista completa de logs e métricas compatíveis, consulte [Logs and Metrics Supported by Amazon CloudWatch Application Insights](#) (Logs e métricas suportadas pelo Amazon CloudWatch Application Insights).

Informações fornecidas sobre os problemas detectados:

- Um breve resumo do problema
- A data e a hora de início do problema
- A gravidade do problema: High/Medium/Low (Alta/média/baixa)
- O status do problema detectado: In-progress/Resolved (Em andamento/resolvido)
- Insights: insights gerados automaticamente sobre o problema detectado e a possível causa
- Feedback sobre os insights: o feedback que você forneceu sobre a utilidade dos insights gerados pelo CloudWatch Application Insights para .NET e SQL Server
- Observações relacionadas: uma visão detalhada das anomalias da métrica e dos trechos do erro de logs relevantes relacionados ao problema em vários componentes da aplicação

Feedback

É possível fornecer feedback em relação aos insights gerados automaticamente sobre problemas detectados designando-os como úteis ou não úteis. Seu feedback sobre os insights com o diagnóstico da aplicação (anomalias da métrica e exceções de log) são usados para melhorar a futura detecção de problemas semelhantes.

Para obter mais informações, consulte a documentação [CloudWatch Application Insights](#) (Insights sobre aplicações do CloudWatch) no Guia do usuário do Amazon CloudWatch.

Redes no Amazon EC2

A Amazon VPC permite que você execute recursos da AWS, como as instâncias do Amazon EC2, em uma rede virtual dedicada à conta da AWS, conhecida como uma nuvem virtual privada (VPC). Ao executar uma instância, você pode selecionar uma sub-rede na VPC. A instância é configurada com uma interface de rede primária, que é uma placa de rede virtual lógica. A instância recebe um endereço IP privado primário do endereço IPv4 da sub-rede e é atribuída à interface da rede primária.

Você pode controlar se a instância recebe um endereço IP público do grupo da Amazon de endereços IP públicos. O endereço IP público de uma instância é associado à sua instância somente até que ela seja interrompida ou encerrada. Se você precisar de um endereço IP público persistente, poderá alocar um endereço IP elástico para a sua conta AWS e associá-lo a uma instância ou uma interface de rede. Um endereço IP elástico permanece associado à sua conta AWS até que você o libere e possa movê-lo de uma instância à outra, conforme necessário. Você pode trazer o seu próprio intervalo de endereços IP para sua conta AWS, onde ele aparece como um grupo de endereços e, em seguida, alocar endereços IP elásticos do seu grupo de endereços.

Para aumentar a performance da rede e reduzir a latência, você pode executar instâncias em um grupo de posicionamento. Você pode obter uma performance significativamente superior de pacotes por segundo (PPS) usando redes aprimoradas. Você pode acelerar aplicações de computação e machine learning de alta performance usando um Elastic Fabric Adapter (EFA), que é um dispositivo de rede que pode ser anexado a um tipo de instância compatível.

Recursos

- [Regiões e zonas \(p. 942\)](#)
- [Endereçamento IP de instâncias do Amazon EC2 \(p. 956\)](#)
- [Traga seus próprios endereços IP \(BYOIP\) no Amazon EC2 \(p. 972\)](#)
- [Atribuição de prefixos a interfaces de rede do Amazon EC2 \(p. 981\)](#)
- [Endereços IP elásticos \(p. 993\)](#)
- [Interfaces de rede elástica \(p. 1002\)](#)
- [Largura de banda de rede de instâncias do Amazon EC2 \(p. 1026\)](#)
- [Rede avançada no Windows \(p. 1028\)](#)
- [Grupos de posicionamento \(p. 1044\)](#)
- [Unidade de transmissão máxima \(MTU\) de rede para a instância do EC2 \(p. 1056\)](#)
- [Nuvens privadas virtuais \(p. 1060\)](#)
- [Portas e protocolos para imagens de máquina da Amazon \(AMIs\) do Windows \(p. 1061\)](#)
- [EC2-Classic \(p. 1099\)](#)

Regiões e zonas

O Amazon EC2 está hospedado em vários locais no mundo todo. Esses locais são compostos por regiões, zonas de disponibilidade, Local Zones, AWS Outposts e zonas do Wavelength. Cada região é uma área geográfica separada.

- As zonas de disponibilidade são vários locais isolados dentro de cada região.
- As Local Zones fornecem a capacidade de colocar recursos, como computação e armazenamento, em vários locais mais próximos dos usuários finais.
- O AWS Outposts leva serviços, infraestrutura e modelos operacionais nativos da AWS a praticamente qualquer datacenter, espaço de colocalização ou on-premises.

- As zonas do Wavelength permitem que os desenvolvedores criem aplicações que oferecem baixíssimas latências para dispositivos 5G e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação.

AWSA opera datacenters de última geração e altamente disponíveis. Embora sejam raras, podem ocorrer falhas que afetam a disponibilidade das instâncias que estão no mesmo local. Se você hospedar todas as suas instâncias em um único local afetado por uma falha, nenhuma delas ficará disponível.

Para ajudar a determinar qual implantação é melhor para você, consulte as [AWS Wavelength Perguntas frequentes](#).

Tópicos

- [Regions \(p. 943\)](#)
- [Zonas de disponibilidade \(p. 947\)](#)
- [Local Zones \(p. 949\)](#)
- [Zonas do Wavelength \(p. 953\)](#)
- [AWS Outposts \(p. 955\)](#)

Regions

Cada região do Amazon EC2 é projetada para ser isolada das outras regiões do Amazon EC2. Isso proporciona a maior tolerância a falhas e estabilidade possível.

Ao visualizar os recursos, você vê apenas os recursos que estão vinculados à região especificada. Isso ocorre porque as regiões são isoladas entre si e nós não replicamos os recursos entre regiões automaticamente.

Ao executar uma instância, você deve selecionar uma AMI que esteja na mesma região. Se a AMI estiver em outra região, você poderá copiar a AMI para a região que está usando. Para obter mais informações, consulte [Copiar um AMI \(p. 120\)](#).

Observe que há uma cobrança para a transferência de dados entre regiões. Para obter mais informações, consulte [Definição de preços do Amazon EC2 – Transferência de dados](#).

Tópicos

- [Regiões disponíveis \(p. 943\)](#)
- [Regiões e endpoints \(p. 945\)](#)
- [Descreva suas regiões \(p. 945\)](#)
- [Obter o nome da região \(p. 946\)](#)
- [Especificar a região para um recurso \(p. 946\)](#)

Regiões disponíveis

Sua conta determina as regiões que estão disponíveis para você.

- Uma conta da AWS fornece várias regiões para que você possa executar instâncias do Amazon EC2 em locais que atendam às suas necessidades. Por exemplo, talvez você queira executar instâncias na Europa para estar mais próximo de seus clientes europeus ou para cumprir requisitos legais.
- Uma conta AWS GovCloud (Oeste dos EUA) fornece acesso somente à região AWS GovCloud (Oeste dos EUA) e à região AWS GovCloud (Leste dos EUA). Para obter mais informações, consulte [AWS GovCloud \(EUA\)](#).

- Uma conta da Amazon AWS (China) fornece acesso somente às regiões Pequim e Ningxia. Para obter mais informações, consulte [AWS na China](#).

A tabela a seguir lista as regiões fornecidas por uma conta da AWS. Não é possível descrever ou acessar regiões adicionais de uma conta da AWS, como a AWS GovCloud (US) Region ou as regiões da China. Para usar uma região introduzida depois de 20 de março de 2019, você deve habilitar a região. Para obter mais informações, consulte [Managing AWS Regions](#) (Gerenciar regiões da AWS) na AWS General Reference (Referência geral da AWS).

Para obter informações sobre as zonas do Wavelength, consulte [Available Wavelength Zones \(Zonas do Wavelength disponíveis\)](#) no Guia do desenvolvedor do AWS Wavelength. Para obter informações sobre as Local Zones disponíveis, consulte [the section called “Local Zones disponíveis” \(p. 950\)](#).

Código	Nome	Status Opt-in
us-east-2	US East (Ohio)	Não obrigatório
us-east-1	Leste dos EUA (Norte da Virgínia)	Não obrigatório
us-west-1	Oeste dos EUA (Norte da Califórnia)	Não obrigatório
us-west-2	Oeste dos EUA (Oregon)	Não obrigatório
af-south-1	Africa (Cape Town)	Obrigatório
ap-east-1	Asia Pacific (Hong Kong)	Obrigatório
ap-south-1	Asia Pacific (Mumbai)	Não obrigatório
ap-northeast-3	Asia Pacific (Osaka)	Não obrigatório
ap-northeast-2	Asia Pacific (Seoul)	Não obrigatório
ap-southeast-1	Ásia-Pacífico (Cingapura)	Não obrigatório
ap-southeast-2	Ásia-Pacífico (Sydney)	Não obrigatório
ap-northeast-1	Ásia-Pacífico (Tóquio)	Não obrigatório
ca-central-1	Canada (Central)	Não obrigatório
eu-central-1	Europe (Frankfurt)	Não obrigatório
eu-west-1	Europa (Irlanda)	Não obrigatório
eu-west-2	Europe (London)	Não obrigatório
eu-south-1	Europe (Milan)	Obrigatório
eu-west-3	Europe (Paris)	Não obrigatório
eu-north-1	Europe (Stockholm)	Não obrigatório
me-south-1	Middle East (Bahrain)	Obrigatório
sa-east-1	América do Sul (São Paulo)	Não obrigatório

Para obter mais informações, consulte [Infraestrutura global da AWS](#).

O número e o mapeamento de zonas de disponibilidade por região podem variar entre contas da AWS. Para obter uma lista de zonas de disponibilidade que estão disponíveis para sua conta, você pode usar o console do Amazon EC2 ou a interface de linha de comando. Para obter mais informações, consulte [Descreva suas regiões \(p. 945\)](#).

Regiões e endpoints

Ao trabalhar com uma instância usando a interface de linha de comando ou ações de API, é necessário especificar seu endpoint regional. Para obter mais informações sobre as regiões e os endpoints para o Amazon EC2, consulte [Endpoints e cotas do Amazon EC2](#) no Amazon Web Services General Reference.

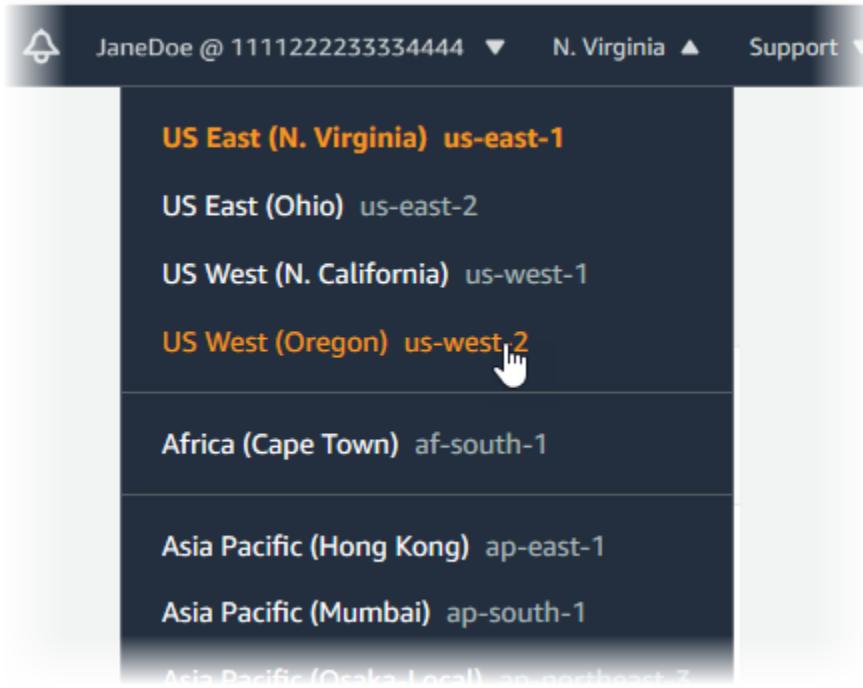
Para obter mais informações sobre os endpoints e os protocolos em AWS GovCloud (Oeste dos EUA), consulte [AWS GovCloud \(US-West\) Endpoints](#) (Endpoints da AWS GovCloud (Oeste dos EUA)) no AWS GovCloud (US) User Guide (Manual do usuário da AWS GovCloud (EUA)).

Descreva suas regiões

Você pode usar o console do Amazon EC2 ou a interface da linha de comando para determinar quais regiões estão disponíveis para sua conta. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

Como localizar suas regiões usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, visualize as opções no seletor de regiões.



3. Seus recursos do EC2 para esta região são exibidos no EC2 Dashboard (Painel do EC2) na seção Resources (Recursos).

Como localizar suas regiões usando a AWS CLI

- Use o comando `describe-regions` como a seguir para descrever as regiões habilitadas para sua conta.

```
aws ec2 describe-regions
```

Para descrever todas as regiões, incluindo as regiões que estão desabilitadas para sua conta, adicione a opção --all-regions da seguinte forma.

```
aws ec2 describe-regions --all-regions
```

Como localizar suas regiões usando a AWS Tools for Windows PowerShell

- Use o comando [Get-EC2Region](#) como a seguir para descrever as regiões de sua conta.

```
PS C:\> Get-EC2Region
```

Obter o nome da região

Você pode usar a API Amazon Lightsail para exibir o nome de uma região.

Como exibir o nome da região usando a AWS CLI

- Use o comando [get-regions](#) da seguinte maneira para descrever o nome da região especificada.

```
aws lightsail get-regions --query "regions[?name=='region-name'].displayName" --output text
```

O exemplo a seguir retorna o nome da região us-east-2.

```
aws lightsail get-regions --query "regions[?name=='us-east-2'].displayName" --output text
```

Esta é a saída:

```
Ohio
```

Especificar a região para um recurso

Sempre que você cria um recurso do Amazon EC2, é possível especificar a região para o recurso. Você pode especificar a região para um recurso usando o AWS Management Console ou a linha de comando.

Considerations

Alguns recursos da AWS podem não estar disponíveis em todas as regiões. Certifique-se de que você pode criar os recursos necessários nas regiões desejadas antes de executar uma instância.

Para especificar a região para um recurso usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Use o seletor de regiões na barra de navegação.

Para especificar a região padrão usando a linha de comando

Você pode definir o valor de uma variável de ambiente para o endpoint regional desejado (por exemplo, <https://ec2.us-east-2.amazonaws.com>):

- `AWS_DEFAULT_REGION` (AWS CLI)
- `Set-AWSDefaultRegion` (AWS Tools for Windows PowerShell)

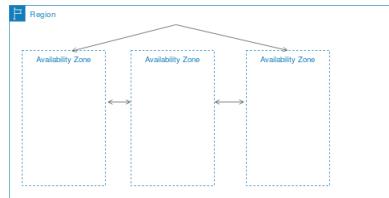
Como alternativa, você pode usar o código `--region` (AWS CLI) ou a opção da linha de comando `-Region` (AWS Tools for Windows PowerShell) com cada comando individual. Por exemplo, `--region us-east-2`.

Para obter mais informações sobre os endpoints para o Amazon EC2, consulte [Endpoints do Amazon Elastic Compute Cloud](#).

Zonas de disponibilidade

Cada região contém vários locais isolados conhecidos como zonas de disponibilidade. Quando você executa uma instância, pode selecionar uma zona de disponibilidade ou deixar-nos escolher uma para você. Se você distribuir suas instâncias em várias zonas de disponibilidade e uma instância falhar, poderá projetar sua aplicação para que uma instância em outra zona de disponibilidade possa processar solicitações.

O diagrama a seguir ilustra várias zonas de disponibilidade em uma região da AWS.



Você também pode usar endereços IP elásticos para mascarar a falha de uma instância em uma zona de disponibilidade rapidamente, remapeando o endereço para uma instância em outra zona de disponibilidade. Para obter mais informações, consulte [Endereços IP elásticos \(p. 993\)](#).

Uma zona de disponibilidade é representada por um código de região seguido por um identificador de letra, por exemplo, `us-east-1a`. Para garantir a distribuição de recursos entre as zonas de disponibilidade de uma região, mapeamos as zonas de disponibilidade de forma independente para os nomes de cada conta da AWS. Por exemplo, a zona de disponibilidade da `us-east-1a` para sua conta da AWS pode não ter o mesmo local que a `us-east-1a` de outra conta da AWS.

Para coordenar as zonas de disponibilidade entre contas, você deve usar o ID da AZ que é um identificador exclusivo e consistente para uma zona de disponibilidade. Por exemplo, `use1-az1` é um ID de AZ para a região `us-east-1` e tem o mesmo local em cada conta da AWS.

É possível visualizar os IDs de AZs para determinar o local de recursos em uma conta em relação aos recursos em outra conta. Por exemplo, se você compartilhar uma sub-rede na zona de disponibilidade com o ID de AZ `use-az2` com outra conta, essa sub-rede estará disponível para essa conta na zona de disponibilidade cujo ID de AZ também é `use-az2`. O ID da AZ de cada VPC e sub-rede é exibido no console da Amazon VPC. Para obter mais informações, consulte [Trabalhar com VPCs compartilhadas](#) no Guia do usuário da Amazon VPC.

Como as zonas de disponibilidade crescem com o tempo, nossa capacidade de expandi-las pode se tornar restrita. Se isso acontecer, nós poderemos impedir que você execute uma instância em uma zona de disponibilidade restrita a menos que você já tenha uma instância naquela zona de

disponibilidade. Finalmente, também podemos remover a zona de disponibilidade restrita da lista de zonas de disponibilidade para novas contas. Portanto, sua conta pode ter um número diferente de zonas de disponibilidade disponíveis em uma região em comparação a outra conta.

Tópicos

- [Descrever suas zonas de disponibilidade \(p. 948\)](#)
- [Executar instâncias em uma zona de disponibilidade \(p. 948\)](#)
- [Migrar uma instância para outra zona de disponibilidade \(p. 949\)](#)

Descrever suas zonas de disponibilidade

Você pode usar o console do Amazon EC2 ou a interface da linha de comando para determinar quais zonas de disponibilidade estão disponíveis para sua conta. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

Como localizar suas zonas de disponibilidade usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, visualize as opções no seletor de regiões.
3. No painel de navegação, escolha EC2 Dashboard.
4. As zonas de disponibilidade são listadas em Service health (Integridade do serviço), Zone status (Status da zona).

Como localizar suas zonas de disponibilidade usando a AWS CLI

1. Use o comando `describe-availability-zones` como a seguir para descrever as zonas de disponibilidade na região especificada.

```
aws ec2 describe-availability-zones --region region-name
```

2. Use o comando `describe-availability-zones` conforme mostrado a seguir para descrever as zonas de disponibilidade independentemente do status da opção.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Como localizar suas zonas de disponibilidade usando a AWS Tools for Windows PowerShell

Use o comando `Get-EC2AvailabilityZone` como a seguir para descrever as zonas de disponibilidade na região especificada.

```
PS C:\> Get-EC2AvailabilityZone -Region region-name
```

Executar instâncias em uma zona de disponibilidade

Ao executar uma instância, selecione uma região que deixe suas instâncias mais próximas de clientes específicos ou cumpra os requisitos legais ou outros. Ao iniciar as instâncias em zonas de disponibilidade separadas, você pode proteger suas aplicações contra falhas em um único local.

Quando você executa uma instância, é possível especificar uma zona de disponibilidade na região que está usando. Se você não especificar uma zona de disponibilidade, selecionaremos uma zona de

disponibilidade para você. Ao executar instâncias iniciais, recomendamos aceitar a zona de disponibilidade padrão. Assim, podemos selecionar a melhor zona de disponibilidade para você de acordo com a integridade do sistema e a capacidade disponível. Se você executar instâncias adicionais, especifique somente uma zona se as novas instâncias precisarem estar próximas ou separadas de suas instâncias em execução.

Migrar uma instância para outra zona de disponibilidade

Se necessário, você poderá migrar uma instância de uma zona de disponibilidade para outra. Por exemplo, digamos que você esteja tentando modificar o tipo de sua instância e não podemos executar uma instância do novo tipo de instância na zona de disponibilidade atual. Nesse caso, você poderá migrar a instância para uma zona de disponibilidade onde possamos executar esse tipo de instância.

O processo de migração envolve:

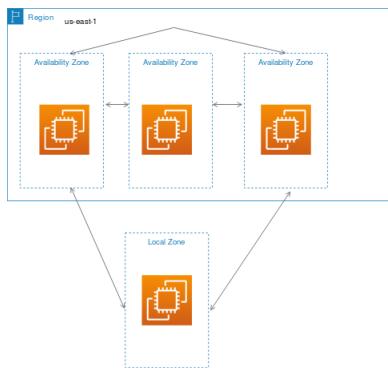
- Criação de uma AMI da instância original
- Execução de uma instância na nova zona de disponibilidade
- Atualização da configuração da nova instância, conforme mostrado no procedimento a seguir

Para migrar uma instância para outra zona de disponibilidade

1. Crie um AMI a partir da instância. O procedimento depende do sistema operacional e do tipo de volume do dispositivo raiz para a instância. Para obter mais informações, consulte a documentação correspondente a seu sistema operacional e volume do dispositivo raiz:
 - [Criar uma AMI do Linux baseada em Amazon EBS](#)
 - [Criar uma AMI em Linux com armazenamento de instâncias](#)
 - [Criar uma AMI do Windows personalizada](#)
2. Se for necessário preservar o endereço IPv4 privado da instância, você deverá excluir a sub-rede na zona de disponibilidade atual e criar uma sub-rede na nova zona de disponibilidade com o mesmo intervalo de endereço IPv4 que a sub-rede original. Observe que você deve encerrar todas as instâncias em uma sub-rede antes de excluí-la. Portanto, você deve criar AMIs de todas as instâncias em sua sub-rede de modo que possa mover todas as instâncias na sub-rede atual para a nova sub-rede.
3. Execute uma instância da AMI que você acabou de criar, especificando a nova zona de disponibilidade ou a sub-rede. Você pode usar o mesmo tipo de instância que a instância original ou selecionar um novo tipo de instância. Para obter mais informações, consulte [Executar instâncias em uma zona de disponibilidade \(p. 948\)](#).
4. Se a instância original tiver um endereço IP elástico associado, associe-o à nova instância. Para obter mais informações, consulte [Dissociar um endereço IP elástico \(p. 998\)](#).
5. Se a instância original for uma Instância reservada, altere a zona de disponibilidade da sua reserva. Se você também tiver mudado o tipo de instância, poderá alterar o tipo de instância para sua reserva. Para obter mais informações, consulte [Enviar solicitações de modificação \(p. 291\)](#).
6. (Opcional) Encerre a instância original. Para obter mais informações, consulte [Como encerrar uma instância \(p. 475\)](#).

Local Zones

Uma Local Zone é uma extensão de uma região da AWS na proximidade geográfica de seus usuários. As Local Zones têm suas próprias conexões com a Internet e são compatíveis com o AWS Direct Connect para que os recursos criados em uma Local Zone possam atender usuários locais com comunicações de baixa latência. Para obter mais informações, consulte [Local ZonesAWS](#).



Uma Local Zone é representada por um código de região da seguido por um identificador que indica a localização, por exemplo, `us-west-2-1ax-1a`. Para obter mais informações, consulte [Local Zones disponíveis \(p. 950\)](#).

Para usar uma Local Zone, é necessário ativá-la primeiro. Para obter mais informações, consulte [the section called “Optar por Local Zones” \(p. 952\)](#). Depois, crie uma sub-rede na Local Zone. Por fim, inicie qualquer um dos seguintes recursos na sub-rede da Local Zone, para que suas aplicações fiquem mais próximas dos usuários finais:

- Instâncias do Amazon EC2
- Volumes do Amazon EBS
- Amazon ECS
- Amazon EKS
- Gateways da Internet

Além da lista acima, os seguintes recursos estão disponíveis nas Local Zones de Los Angeles.

- Servidores de arquivos do Amazon FSx
- Elastic Load Balancing
- Amazon EMR
- Amazon ElastiCache
- Amazon Relational Database Service
- Dedicated Hosts

Tópicos

- [Local Zones disponíveis \(p. 950\)](#)
- [Descreva suas Local Zones \(p. 951\)](#)
- [Optar por Local Zones \(p. 952\)](#)
- [Executar instâncias em uma Local Zone \(p. 952\)](#)

Local Zones disponíveis

A tabela a seguir lista as Local Zones disponíveis por Região pai. Para obter informações sobre como fazer login, consulte [the section called “Optar por Local Zones” \(p. 952\)](#).

Local Zones do Leste dos EUA (Norte da Virgínia)

Esta tabela lista as Local Zones no Leste dos EUA (Norte da Virgínia):

Região-principal	Nome da Zona	Local
Leste dos EUA (Norte da Virgínia)	us-east-1-bos-1a	Boston ()
Leste dos EUA (Norte da Virgínia)	us-east-1-chi-1a	Chicago
Leste dos EUA (Norte da Virgínia)	us-east-1-dfw-1a	Dallas
Leste dos EUA (Norte da Virgínia)	us-east-1-iah-1a	HOUSTON
Leste dos EUA (Norte da Virgínia)	us-east-1-mci-1a	Cidade de Kansas
Leste dos EUA (Norte da Virgínia)	us-east-1-mia-1a	Miami
Leste dos EUA (Norte da Virgínia)	us-east-1-msp-1a	Minneapolis
Leste dos EUA (Norte da Virgínia)	us-east-1-phl-1a	Filadélfia

Local Zones do Oeste dos EUA (Oregon)

Esta tabela lista Local Zones no Oeste dos EUA (Oregon):

Região-principal	Nome da Zona	Local
Oeste dos EUA (Oregon)	us-west-2-den-1a	Denver
Oeste dos EUA (Oregon)	us-west-2-lax-1a	Los Angeles
Oeste dos EUA (Oregon)	us-west-2-lax-1b	Los Angeles

Descreva suas Local Zones

Você pode usar o console do Amazon EC2 ou a interface da linha de comando para determinar quais Local Zones estão disponíveis para sua conta. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

Como localizar suas Local Zones usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, visualize as opções no seletor de regiões.
3. No painel de navegação, escolha EC2 Dashboard.
4. As Local Zones estão listadas em Service health (Integridade do serviço), Zone status (Status da zona).

Para localizar suas Local Zones usando a AWS CLI

1. Use o comando `describe-availability-zones` como a seguir para descrever as Local Zones na região especificada.

```
aws ec2 describe-availability-zones --region region-name
```

2. Use o comando `describe-availability-zones` como a seguir para descrever os Local Zones independentemente de estarem habilitados.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Para localizar suas Local Zones usando a AWS Tools for Windows PowerShell

Use o comando [Get-EC2AvailabilityZone](#) como a seguir para descrever as Local Zones na região especificada.

```
PS C:\> Get-EC2AvailabilityZone -Region region-name
```

Optar por Local Zones

Antes de especificar uma Local Zone para um recurso ou serviço, é necessário optar por Local Zones.

Consideration

Alguns recursos da AWS podem não estar disponíveis em todas as regiões. Verifique se você pode criar os recursos necessários nas regiões ou Local Zones desejadas antes de executar uma instância em uma Local Zone específica.

Para optar por Local Zones usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No canto superior esquerdo da página, selecione New EC2 Experience (Nova experiência do EC2). Não é possível concluir essa tarefa usando a experiência de console antiga.
3. No seletor de região na barra de navegação, selecione a região para a Local Zone.
4. No painel de navegação, escolha EC2 Dashboard.
5. No canto superior direito da página, escolha Account Attributes (Atributos da conta), Zones (Zonas).
6. Escolha Gerenciar.
7. Em Zone group (Grupo de zonas), escolha Enabled (Habilitado).
8. Escolha Update zone group (Atualizar grupo de zonas).

Para optar por Local Zones usando o AWS CLI

- Use o comando [modify-availability-zone-group](#).

Executar instâncias em uma Local Zone

Ao executar uma instância, você pode especificar uma sub-rede que está em uma Local Zone. É possível alocar os endereços IP de um grupo de bordas de rede: Um grupo de bordas de rede é um conjunto exclusivo de zonas de disponibilidade, Local Zones ou zonas do Wavelength, das quais a AWS anuncia endereços IP, por exemplo, us-west-2-lax-1a.

É possível alocar os endereços IP de um grupo de bordas de rede:

- Endereços IPv4 elásticos fornecidos pela Amazon
- Endereços da VPC IPv6 fornecidos pela Amazon

Para executar instâncias em uma Local Zone:

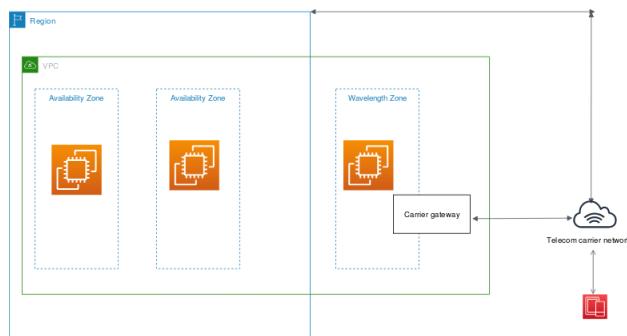
1. Habilite as Local Zones. Para obter mais informações, consulte [Optar por Local Zones \(p. 952\)](#).

2. Crie uma VPC em uma região que seja compatível com a Local Zone. Para obter mais informações, consulte [Criar uma VPC](#) no Guia do usuário da Amazon VPC.
3. Crie uma sub-rede. Selecione a Local Zone ao criar a sub-rede. Para obter mais informações, consulte [Criar uma sub-rede na VPC](#) no Guia do usuário da Amazon VPC.
4. Execute uma instância e selecione a sub-rede que você criou na Local Zone. Para obter mais informações, consulte [Executar sua instância \(p. 417\)](#).

Zonas do Wavelength

AWS WavelengthO permite que os desenvolvedores criem aplicações que oferecem baixíssimas latências para dispositivos móveis e usuários finais. O Wavelength implanta os serviços de armazenamento e computação padrão da AWS até a borda das redes 5G de operadoras de telecomunicação. Os desenvolvedores podem estender uma nuvem privada virtual (VPC) para uma ou mais zonas do Wavelength e usar os recursos da AWS, como instâncias do Amazon EC2, para executar aplicações que exigem baixíssima latência e uma conexão com produtos da AWS na região.

Uma Wavelength Zone é uma zona isolada no local da transportadora em que a infraestrutura de Wavelength é implantada. As zonas de Wavelength estão vinculadas a uma região. Uma zona de Wavelength é uma extensão lógica de uma região e é gerenciada pelo plano de controle na região.



Uma zona de Wavelength é representada por um código de região seguido por um identificador que indica a zona de Wavelength, por exemplo, us-east-1-wl1-bos-wlz-1.

Para usar uma zona de Wavelength, você deve primeiro escolher a zona. Para obter mais informações, consulte [the section called “Habilitar zonas de Wavelength” \(p. 954\)](#). Em seguida, crie uma sub-rede na zona de Wavelength. Por fim, inicie seus recursos na sub-rede das zonas de Wavelength, para que suas aplicações estejam mais próximas dos usuários finais.

As Wavelength Zones não estão disponíveis em todas as regiões. Para obter informações sobre as regiões compatíveis com as zonas do Wavelength consulte [Zonas do Wavelength disponíveis](#) no Guia do desenvolvedor da AWS Wavelength.

Tópicos

- [Descreva suas zonas de Wavelength \(p. 953\)](#)
- [Habilitar zonas de Wavelength \(p. 954\)](#)
- [Executar instâncias em uma zona de Wavelength \(p. 955\)](#)

Descreva suas zonas de Wavelength

Você pode usar o console do Amazon EC2 ou a interface da linha de comando para determinar quais zonas de Wavelength estão disponíveis para sua conta. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

Como localizar suas zonas de Wavelength usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, visualize as opções no seletor de regiões.
3. No painel de navegação, escolha EC2 Dashboard.
4. As zonas de Wavelength estão listadas em Service health (Integridade do serviço), Zone status (Status da zona).

Como localizar suas zonas de Wavelength usando a AWS CLI

1. Use o comando `describe-availability-zones` como a seguir para descrever as zonas de Wavelength na região especificada.

```
aws ec2 describe-availability-zones --region region-name
```

2. Use o comando `describe-availability-zones` como a seguir para descrever as zonas de Wavelength independentemente do status da opção.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Como localizar a zona de Wavelength usando o AWS Tools for Windows PowerShell

Use o comando `Get-EC2AvailabilityZone` como a seguir para descrever as Wavelength Zones na região especificada.

```
PS C:\> Get-EC2AvailabilityZone -Region region-name
```

Habilitar zonas de Wavelength

Antes de especificar uma zona do Wavelength para um recurso ou serviço, é necessário aceitar as zonas do Wavelength.

Considerations

- Alguns recursos da AWS não estão disponíveis em todas as regiões. Certifique-se de que você pode criar os recursos necessários na região ou zona de Wavelength desejada antes de executar uma instância em uma zona de Wavelength específica.

Como ativar zonas de Wavelength usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No canto superior esquerdo da página, selecione New EC2 Experience (Nova experiência do EC2). Não é possível concluir essa tarefa usando a experiência de console antiga.
3. No seletor de região na barra de navegação, selecione a região para a zona de Wavelength.
4. No painel de navegação, escolha EC2 Dashboard.
5. No canto superior direito da página, escolha Account Attributes (Atributos da conta), Zones (Zonas).
6. Em Wavelength Zones (Zonas do Wavelength), escolha Manage (Gerenciar) para a zona do Wavelength.
7. Escolha Enable (Habilitar).
8. Escolha Update zone group (Atualizar grupo de zonas).

Como habilitar zonas de Wavelength usando a AWS CLI

Use o comando [modify-availability-zone-group](#).

Executar instâncias em uma zona de Wavelength

Ao executar uma instância, você pode especificar uma sub-rede que está em uma zona de Wavelength. Você também aloca o endereço IP de uma operadora de um grupo de bordas de rede, que é um conjunto exclusivo de zonas de disponibilidade, Local Zones ou zonas do Wavelength, das quais a AWS anuncia endereços IP, por exemplo, us-east-1-wl1-bos-wlz-1.

Para obter informações sobre como executar uma instância em uma zona do Wavelength, consulte [Conceitos básicos do AWS Wavelength Wavelength](#) no Guia do desenvolvedor do AWS Wavelength.

AWS Outposts

O AWS Outposts é um serviço totalmente gerenciado que estende a infraestrutura, os serviços, as APIs e as ferramentas da AWS no local do cliente. Ao fornecer acesso local à infraestrutura gerenciada pela AWS, o AWS Outposts permite que os clientes criem e executem aplicações on-premises usando as mesmas interfaces de programação que nas regiões da AWS, ao mesmo tempo que usam recursos locais de computação e armazenamento para menor latência e necessidades de processamento de dados locais.

Um Outpost é um grupo de capacidade de computação e armazenamento da AWS implantado em um local do cliente. A AWS opera, monitora e gerencia essa capacidade como parte de uma região da AWS. Você pode criar sub-redes no Outpost e especificá-las ao criar recursos da AWS, como instâncias do EC2, volumes do EBS, clusters do ECS e instâncias do RDS. As instâncias nas sub-redes do Outpost se comunicam com outras instâncias na região da AWS usando endereços IP privados, tudo na mesma VPC.

Para começar a usar o AWS Outposts, você deve criar um Outpost e solicitar capacidade para o Outpost. Para obter mais informações sobre configurações de Outposts, consulte [nossa catálogo](#). Depois que o equipamento do Outpost for instalado, a capacidade de computação e armazenamento estará disponível quando você executar instâncias do Amazon EC2 e criar volumes do Amazon EBS no Outpost.

Executar instâncias em um Outpost

Você pode executar instâncias do EC2 na sub-rede do Outpost que você criou. Os grupos de segurança controlam o tráfego de entrada e de saída de instâncias em uma sub-rede do Outpost, como fazem para instâncias em uma sub-rede de zona de disponibilidade. Para conectar-se a uma instância do EC2 em uma sub-rede do Outpost, você pode especificar um par de chaves ao executar a instância, como o faz para instâncias em uma sub-rede de zona de disponibilidade.

O volume raiz deve ser de 30 GB ou menor. Você pode especificar volumes de dados no mapeamento de dispositivo de bloco da AMI ou na instância para fornecer armazenamento adicional. Para eliminar blocos não utilizados do volume de inicialização, consulte [Como criar volumes de EBS esparsos](#) no blog da rede de parceiros da AWS.

Recomendamos aumentar o tempo limite de NVMe para o volume raiz. Para obter mais informações, consulte [Tempo limite de operação de E/S \(p. 1440\)](#).

Para obter informações sobre como criar um Outpost, consulte [Get started with AWS Outposts \(Conceitos básicos do Outpost\)](#) no Guia do Usuário AWS Outposts.

Criar um volume em um Outpost

Você pode criar volumes do EBS na sub-rede do Outpost que você criou. Ao criar o volume, especifique o nome de recurso da Amazon (ARN) do Outpost.

O seguinte comando [create-volume](#) cria um volume vazio de 50 GB no Outpost especificado.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

Você pode modificar dinamicamente o tamanho dos volumes gp2 Amazon EBS sem desanexá-los. Para obter mais informações sobre como modificar um volume sem desanexá-los, consulte [Solicitar modificações para seus volumes do EBS \(p. 1411\)](#).

Endereçamento IP de instâncias do Amazon EC2

O Amazon EC2 e a Amazon VPC oferecem suporte aos protocolos de endereçamento IPv4 e IPv6. Por padrão, o Amazon EC2 e a Amazon VPC usam o protocolo de endereçamento IPv4. Não é possível desabilitar esse comportamento. Ao criar uma VPC, você deve especificar um bloco CIDR IPv4 (um intervalo de endereços IPv4 privados). Opcionalmente, você pode atribuir um bloco CIDR IPv6 à VPC e às sub-redes e atribuir endereços IPv6 desse bloco a instâncias na sub-rede. Os endereços IPv6 são acessíveis pela Internet. Para obter mais informações sobre IPv6, consulte [Endereçamento IP na sua VPC](#) no Guia do usuário da Amazon VPC.

Tópicos

- [Endereços IPv4 privados e nomes de host DNS internos \(p. 956\)](#)
- [Endereços IPv4 públicos e nomes de host DNS externos \(p. 957\)](#)
- [Endereços IP elásticos \(IPv4\) \(p. 958\)](#)
- [Servidor DNS da Amazon \(p. 958\)](#)
- [Endereços IPv6 \(p. 958\)](#)
- [Trabalhar com os endereços IPv4 para as instâncias \(p. 959\)](#)
- [Trabalhar com os endereços IPv6 para as instâncias \(p. 962\)](#)
- [Vários endereços IP \(p. 964\)](#)

Endereços IPv4 privados e nomes de host DNS internos

Um endereço IPv4 privado é um endereço IP que não é acessível pela Internet. Você pode usar endereços IPv4 privados para comunicação entre instâncias na mesma VPC. Para obter mais informações sobre os padrões e as especificações de endereços IPv4 privados, consulte a [RFC 1918](#). Atribuímos os endereços IPv4 privados a instâncias usando o DHCP.

Note

Você pode criar uma VPC com um bloco CIDR publicamente roteável que esteja fora dos intervalos de endereços IPv4 privados especificados na RFC 1918. No entanto, para fins dessa documentação, referimo-nos aos endereços IPv4 privados (ou “endereços IP privados”) como os endereços IP que estão no intervalo CIDR IPv4 da VPC.

Quando você inicia uma instância, alocamos um endereço IPv4 privado para a instância. Cada instância também recebe um nome de host DNS interno que é resolvido para o endereço IPv4 primário, por exemplo, ip-10-251-50-12.ec2.internal. É possível usar o nome de host DNS interno para comunicação entre instâncias na mesma VPC, mas não podemos resolver o nome de host DNS interno fora da VPC.

Uma instância recebe um endereço IP privado primário do intervalo de endereços IPv4 da sub-rede. Para obter mais informações, consulte [Dimensionamento da VPC e da sub-rede](#) no Guia do usuário

da Amazon VPC. Se você não especificar um endereço IP privado primário ao executar a instância, selecionaremos um endereço IP disponível no intervalo IPv4 da sub-rede para você. Cada instância tem uma interface de rede padrão (eth0) que recebe o endereço IPv4 privado primário. Você também pode especificar endereços IPv4 privados adicionais, conhecidos como endereços IPv4 privados secundários. Ao contrário de um endereço IP privado primário, os endereços IP privados secundários podem ser atribuídos novamente de uma instância para outra. Para obter mais informações, consulte [Vários endereços IP \(p. 964\)](#).

Um endereço IPv4 privado, independentemente de ser um endereço primário ou secundário, permanece associado à interface de rede quando a instância é interrompida e reiniciada ou é hibernada e iniciada, e é liberado quando a instância é encerrada.

Endereços IPv4 públicos e nomes de host DNS externos

Um endereço IP público é um endereço IPv4 que é acessível pela Internet. Você pode usar endereços públicos para comunicação entre as instâncias e a Internet.

Cada instância que recebe um endereço IP público também recebe um nome de host DNS externo, por exemplo, ec2-203-0-113-25.compute-1.amazonaws.com. Resolvemos um nome de host DNS externo como o endereço IP público da instância fora da VPC e como o endereço IPv4 privado da instância dentro da VPC. O endereço IP público é mapeado para o endereço IP privado primário por meio da conversão de endereço de rede (NAT). Para obter mais informações, consulte a [RFC 1631: o conversor de endereço de rede \(NAT\) IP](#).

Quando você inicia uma instância em uma VPC padrão, atribuímos a ela um endereço IP público por padrão. Quando você executa uma instância em uma VPC não padrão, a sub-rede tem um atributo que determina se as instâncias executadas naquela sub-rede recebem um endereço IP público do grupo de endereços IPv4 públicos. Por padrão, não atribuímos um endereço IP público a instâncias iniciadas em uma sub-rede não padrão.

Você pode controlar se sua instância recebe um endereço IP público fazendo o seguinte:

- Modificando o atributo de endereçamento IP público da sub-rede. Para obter mais informações, consulte [Modificar o atributo de endereçamento IPv4 público para a sub-rede](#) no Guia do usuário da Amazon VPC.
- Habilitando ou desabilitando o recurso de endereçamento IP público durante a execução da instância, o que substitui o atributo de endereçamento IP público da sub-rede. Para obter mais informações, consulte [Atribuir um endereço IPv4 público durante a execução da instância \(p. 961\)](#).

Um endereço IP público é atribuído à instância no grupo de endereços IPv4 públicos da Amazon e não está associado à sua conta da AWS. Quando um endereço IP público é desassociado da instância, ele é liberado de volta para o grupo de endereços IPv4 públicos, e você não pode reutilizá-lo.

Você não pode associar ou desassociar manualmente um endereço IP público (IPv4) da instância. Em vez disso, em certos casos, liberamos o endereço IP público de sua instância ou atribuímos um novo:

- Liberamos o endereço IP público da instância quando ela é interrompida, hibernada ou encerrada. Sua instância interrompida ou hibernada recebe um novo endereço IP público quando é iniciada.
- Liberamos o endereço IP público de sua instância ao associar um endereço IP elástico a ela. Quando você desassocia o endereço IP elástico da instância, ela recebe um novo endereço IP público.
- Se o endereço IP público da instância em uma VPC foi liberado, ela não receberá um novo se houver mais de uma interface de rede anexada à instância.
- Se o endereço IP público da instância for liberado enquanto houver um endereço IP privado secundário associado a um endereço IP elástico, a instância não receberá um novo endereço IP público.

Se você precisar de um endereço IP público persistente que possa ser associado às instâncias e das instâncias conforme necessário, use um endereço IP elástico.

Se você usar o DNS dinâmico para mapear um nome DNS existente para o endereço IP público de uma nova instância, poderá demorar até 24 horas para o endereço IP ser propagado via Internet. Como resultado, as novas instâncias não poderão receber tráfego quando as instâncias encerradas continuarem a receber solicitações. Para resolver o problema, use um endereço IP elástico. É possível alocar seu próprio endereço IP elástico e associá-lo à instância. Para obter mais informações, consulte [Endereços IP elásticos \(p. 993\)](#).

Se você atribuir um endereço IP elástico a uma instância, ela receberá um nome de host DNS IPv4 se os nomes de host DNS estiverem habilitados. Para obter mais informações, consulte [Usar DNS com a VPC](#) no Guia do usuário da Amazon VPC.

Note

As instâncias que acessam outras instâncias por meio de seu endereço IP NAT público são cobradas pela transferência de dados regional ou via Internet, dependendo de se as instâncias estão na mesma região.

Endereços IP elásticos (IPv4)

Um endereço IP elástico é um endereço IPv4 público que você pode alocar à sua conta. É possível associá-lo e desassociá-lo de instâncias conforme necessário. Ele é alocado para sua conta até que você opte por liberá-lo. Para obter mais informações sobre endereços IP elásticos e como usá-los, consulte [Endereços IP elásticos \(p. 993\)](#).

Não oferecemos suporte a endereços IP elásticos para IPv6.

Servidor DNS da Amazon

A Amazon fornece um servidor DNS que resolve nomes de host DNS IPv4 fornecidos pela Amazon para endereços IPv4. O servidor DNS da Amazon está localizado na base de seu intervalo de rede VPC mais dois. Para obter mais informações, consulte [Servidor DNS da Amazon](#) no Guia do usuário da Amazon VPC.

Endereços IPv6

Opcionalmente, você pode associar um bloco CIDR IPv6 à VPC e associar blocos CIDR IPv6 às sub-redes. O bloco CIDR IPv6 da VPC é automaticamente atribuído do grupo de endereços IPv6 da Amazon. Você não pode escolher o intervalo você mesmo. Para obter mais informações, consulte um dos tópicos a seguir no Guia do usuário da Amazon VPC.

- [Dimensionamento da VPC e da sub-rede para IPv6](#)
- [Associar um bloco CIDR IPv6 à sua VPC](#)
- [Associar um bloco CIDR IPv6 à sub-rede](#)

Os endereços IPv6 são globalmente exclusivos e, portanto, acessíveis pela Internet. A instância recebe um endereço IPv6 se um bloco CIDR IPv6 estiver associado à VPC e à sub-rede, e se uma das seguintes afirmações for verdadeira:

- A sub-rede está configurada para atribuir automaticamente um endereço IPv6 a uma instância durante a execução. Para obter mais informações, consulte [Modificar o atributo de endereçamento IPv6 público para a sub-rede](#).
- Você atribui um endereço IPv6 à instância durante a execução.

- Você atribui um endereço IPv6 à interface de rede primária da instância após a execução.
- Você atribui um endereço IPv6 a uma interface de rede na mesma sub-rede e anexa a interface de rede à instância após a execução.

Quando a instância recebe um endereço IPv6 durante a execução, o endereço é associado à interface de rede primária (eth0) da instância. Você pode desassociar o endereço IPv6 da interface de rede. Não oferecemos suporte a nomes de host DNS IPv6 da instância.

Um endereço IPv6 persiste quando você interrompe e inicia ou hiberna e inicia a instância, e é liberado quando você encerra a instância. Você não pode atribuir novamente um endereço IPv6 enquanto ele estiver atribuído a outra interface de rede — você deve primeiro cancelar a atribuição.

Você pode atribuir endereços IPv6 adicionais à instância atribuindo-os a uma interface de rede anexada à instância. O número de endereços IPv6 que você pode atribuir a uma interface de rede e o número de interfaces de rede que você pode anexar a uma instância varia de acordo com o tipo de instância. Para obter mais informações, consulte [Endereços IP por interface de rede por tipo de instância \(p. 1004\)](#).

Trabalhar com os endereços IPv4 para as instâncias

É possível atribuir um endereço IPv4 à instância ao executá-la. É possível ver os endereços IPv4 no console nas páginas Instances (Instâncias) ou Network Interfaces (Interfaces de rede).

Tópicos

- [Visualizar os endereços IPv4 \(p. 959\)](#)
- [Atribuir um endereço IPv4 público durante a execução da instância \(p. 961\)](#)

Visualizar os endereços IPv4

Você pode usar o console do Amazon EC2 para visualizar os endereços IPv4 privados, os endereços IPv4 públicos e os endereços IP elásticos das instâncias. Você também pode determinar os endereços IPv4 públicos e privados da instância usando os metadados da instância. Para obter mais informações, consulte [Metadados da instância e dados do usuário \(p. 622\)](#).

O endereço IPv4 público é exibido como uma propriedade da interface de rede no console, mas é mapeado para o endereço IPv4 privado primário por meio da NAT. Portanto, se você inspecionar as propriedades da interface de rede na instância, por exemplo, por meio do `ifconfig` (Linux) ou do `ipconfig` (Windows), o endereço IPv4 público não será exibido. Para determinar o endereço IPv4 público da instância em uma instância, use os metadados da instância.

New console

Para exibir os endereços IPv4 de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. As seguintes informações estão disponíveis na guia Networking (Redes):
 - Public IPv4 address (Endereço IPv4 público): endereço IPv4 público. Se você associou um endereço IP elástico à instância ou à interface de rede primária, esse será o endereço IP elástico.
 - Public IPv4 DNS (DNS IPv4 público): nome do host do DNS externo.
 - Private IPv4 addresses (Endereços IPv4 privados): o endereço IPv4 privado.
 - Private IPv4 DNS (DNS IPv4 privado): nome do host do DNS interno.

- Secondary private IPv4 addresses (Endereços IPv4 privados secundários): todos os endereços IPv4 privados secundários.
 - Endereços IP elásticos — todos os endereços IP elásticos associados.
4. Como alternativa, em Network interfaces (Interfaces de rede) na guia Networking (Redes), selecione o ID da interface da rede primária (por exemplo, eni-123abc456def78901). As seguintes informações estão disponíveis:
- Private DNS (IPv4) (DNS privado (IPv4)): nome do host do DNS interno.
 - Primary private IPv4 IP (IP IPv4 privado primário): endereço IPv4 privado primário.
 - Secondary private IPv4 IPs (IPs IPv4 privados secundários): endereços IPv4 privados secundários.
 - Public DNS (DNS público): nome do host do DNS externo.
 - IPv4 Public IP (IP público IPv4): endereço IPv4 público. Se você associou um endereço IP elástico à instância ou à interface de rede primária, esse será o endereço IP elástico.
 - Elastic IPs (IPs elásticos): todos os endereços IP elásticos associados.

Old console

Para exibir os endereços IPv4 de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias e selecione sua instância.
3. As informações a seguir estão disponíveis na guia Description (Descrição):
 - Private DNS (DNS privado): nome do host DNS interno.
 - Private IPs (IPs privados): endereço IPv4 privado.
 - Secondary private IPs (IPs privados secundários): endereços IPv4 privados secundários.
 - Public DNS (DNS público): nome do host do DNS externo.
 - IPv4 Public IP (IP público IPv4): endereço IPv4 público. Se você associou um endereço IP elástico à instância ou à interface de rede primária, esse será o endereço IP elástico.
 - Elastic IPs (IPs elásticos): todos os endereços IP elásticos associados.
4. Como alternativa, é possível ver os endereços IPv4 da instância usando a interface de rede primária. Em Network interfaces (Interfaces de rede) na guia Description (Descrição), escolha o ID da interface (por exemplo, eni-123abc456def78901). As seguintes informações estão disponíveis:
 - Private DNS (IPv4) (DNS privado (IPv4)): nome do host do DNS interno.
 - Primary private IPv4 IP (IP IPv4 privado primário): endereço IPv4 privado primário.
 - Secondary private IPv4 IPs (IPs IPv4 privados secundários): endereços IPv4 privados secundários.
 - Public DNS (DNS público): nome do host do DNS externo.
 - IPv4 Public IP (IP público IPv4): endereço IPv4 público. Se você associou um endereço IP elástico à instância ou à interface de rede primária, esse será o endereço IP elástico.
 - Elastic IPs (IPs elásticos): todos os endereços IP elásticos associados.

Para exibir os endereços IPv4 de uma instância usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [describe-instances](#) (AWS CLI)

- [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).

Para determinar os endereços IPv4 da instância usando os metadados

1. Conecte-se à sua instância. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
2. Use o comando a seguir para acessar o endereço IP privado:

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
```

3. Use o comando a seguir para acessar o endereço IP público:

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
```

Se um endereço IP elástico estiver associado à instância, o valor retornado será o do endereço IP elástico.

Atribuir um endereço IPv4 público durante a execução da instância

Toda sub-rede tem um atributo que determina se as instâncias executadas nessa sub-rede recebem um endereço IP público. Por padrão, as sub-redes não padrão têm esse atributo definido como false, e as sub-redes padrão têm esse atributo definido como true. Quando você executa uma instância, um recurso de endereçamento IPv4 público também está disponível para controlar se a instância está atribuída a um endereço IPv4 público. Você pode substituir o comportamento padrão do atributo de endereçamento IP da sub-rede. O endereço IPv4 público é atribuído no grupo de endereços IPv4 públicos da Amazon, e é atribuído à interface de rede com o índice de dispositivo de eth0. Esse recurso depende de determinadas condições no momento em que você executa a instância.

Considerações

- Você não pode desassociar manualmente o endereço IP público da instância após a execução. Em vez disso, ele é automaticamente liberado em determinados casos e depois disso você não pode reutilizá-lo. Para obter mais informações, consulte [Endereços IPv4 públicos e nomes de host DNS externos \(p. 957\)](#). Se você precisar de um endereço IP público persistente que possa ser associado ou desassociado à vontade, atribua um endereço IP elástico à instância após a execução. Para obter mais informações, consulte [Endereços IP elásticos \(p. 993\)](#).
- Você não pode atribuir automaticamente um endereço IP público se especificar mais de uma interface de rede. Além disso, você não pode substituir a configuração da sub-rede usando o recurso de atribuição automática de endereço IP público, se especificar uma interface de rede existente para eth0.
- O recurso de endereçamento IP público só está disponível durante a inicialização. No entanto, quer você atribua ou não um endereço IP público à instância durante a execução, você pode associar um endereço IP elástico à instância depois que ela for executada. Para obter mais informações, consulte [Endereços IP elásticos \(p. 993\)](#). Você também pode modificar o comportamento do endereçamento IPv4 público da sub-rede. Para obter mais informações, consulte [Modificar o atributo de endereçamento IPv4 público para a sub-rede](#).

Para habilitar ou desabilitar o recurso de endereçamento IP público usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Launch Instance (Executar instância).
3. Selecione uma AMI e um tipo de instância e escolha Next: Configure Instance Details.

4. Na página Configure Instance Details, em Network, selecione uma VPC. A lista Auto-assign Public IP é exibida. Escolha Enable ou Disable para substituir a configuração padrão da sub-rede.
5. Siga as etapas nas páginas a seguir do assistente para concluir a configuração da instância. Para obter mais informações sobre as opções da configuração do assistente, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#). Na página final Review Instance Launch, reveja suas configurações, e escolha Launch para escolher um par de chaves e executar a instância.
6. Na página Instances, selecione a nova instância e visualize o endereço IP público correspondente no campo IPv4 Public IP no painel de detalhes.

Para habilitar ou desabilitar o recurso de endereçamento IP público usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- Use a opção --associate-public-ip-address ou --no-associate-public-ip-address com o comando `run-instances` (AWS CLI)
- Use o parâmetro `-AssociatePublicIp` com o comando `New-EC2Instance` (AWS Tools for Windows PowerShell)

Trabalhar com os endereços IPv6 para as instâncias

Você pode visualizar os endereços IPv6 atribuídos à instância, atribuir um endereço IPv6 público à instância ou cancelar a atribuição de um endereço IPv6 da instância. É possível visualizar esses endereços no console na página Instances (Instâncias) ou Network Interfaces (Interfaces de rede).

Tópicos

- [Visualizar os endereços IPv6 \(p. 962\)](#)
- [Atribuir um endereço IPv6 a uma instância \(p. 963\)](#)
- [Cancelar a atribuição de um endereço IPv6 de uma instância \(p. 964\)](#)

Visualizar os endereços IPv6

É possível usar o console do Amazon EC2, a AWS CLI e os metadados de instância para visualizar os endereços IPv6 das instâncias.

New console

Para exibir os endereços IPv6 para uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Networking (Redes), localize IPv6 addresses (Endereços IPv6).
5. Como alternativa, em Network interfaces (Interfaces de rede) na guia Networking (Redes), escolha o ID da interface de rede (por exemplo, eni-123abc456def78901). Localize IPv6 IPs (IPs IPv6).

Old console

Para exibir os endereços IPv6 para uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Networking (Redes), localize IPv6 IPs (IPs IPv6).
5. Como alternativa, em Network interfaces (Interfaces de rede) na guia Description (Descrição), escolhaeth0 e depois escolha o ID da interface (por exemplo, eni-123abc456def78901). Localize IPv6 IPs (IPs IPv6).

Para exibir os endereços IPv6 de uma instância usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).

Para exibir os endereços IPv6 de uma instância usando os metadados de instância

1. Conecte-se à sua instância. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
2. Use o comando a seguir para visualizar o endereço IPv6 (você pode obter o endereço MAC em <http://169.254.169.254/latest/meta-data/network/interfaces/macs/>).

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/network/interfaces/
macs/mac-address/ipv6s
```

Atribuir um endereço IPv6 a uma instância

Se a VPC e a sub-rede tiverem blocos CIDR IPv6 associados a elas, você poderá atribuir um endereço IPv6 à instância durante ou após a execução. O endereço IPv6 é atribuído no intervalo de endereços IPv6 da sub-rede e é atribuído à interface de rede com o índice de dispositivo de eth0.

Para atribuir um endereço IPv6 a uma instância durante a execução

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione um AMI e um tipo de instância que possua suporte a IPv6 e selecione Next: Configure Instance Details.
3. Na página Configure Instance Details, em Network, selecione uma VPC, e em Subnet, selecione uma sub-rede. Em Auto-assign IPv6 IP, escolha Habilitar.
4. Siga as etapas restantes no assistente para executar a instância.

Para atribuir um endereço IPv6 a uma instância após a execução

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).

4. Expanda a interface de rede. Em IPv6 addresses (Endereços IPv6), escolha Assign new IP address (Atribuir novo endereço IP). Insira um endereço IPv6 no intervalo da sub-rede ou deixe o campo em branco para permitir que a Amazon escolha um endereço IPv6 para você.
5. Escolha Save (Salvar).

Para atribuir um endereço IPv6 usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- Use a opção `--ipv6-addresses` com o comando [run-instances](#) (AWS CLI)
- Use a propriedade `Ipv6Addresses` para `-NetworkInterface` no comando [New-EC2Instance](#) (AWS Tools for Windows PowerShell)
- [assign-ipv6-addresses](#) (AWS CLI)
- [Register-EC2Ipv6AddressList](#) (AWS Tools for Windows PowerShell)

Cancelar a atribuição de um endereço IPv6 de uma instância

Você pode cancelar a atribuição de um endereço IPv6 de uma instância a qualquer momento.

Para cancelar a atribuição de um endereço IPv6 de uma instância usando o console.

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).
4. Expanda a interface de rede. Em IPv6 addresses (Endereços IPv6), selecione Unassign (Cancelar atribuição) ao lado de endereços IPv6.
5. Escolha Save (Salvar).

Você pode cancelar a atribuição de um endereço IPv6 de uma instância usando a linha de comando.

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [unassign-ipv6-addresses](#) (AWS CLI)
- [Unregister-EC2Ipv6AddressList](#) (AWS Tools for Windows PowerShell).

Vários endereços IP

Você pode especificar vários endereços IPv4 privados e endereços IPv6 para as instâncias. O número de interfaces de rede e de endereços de IPv4 e IPv6 privados que você pode especificar para uma instância depende do tipo da instância. Para obter mais informações, consulte [Endereços IP por interface de rede por tipo de instância \(p. 1004\)](#).

Pode ser útil atribuir vários endereços IP a uma instância na VPC para fazer o seguinte:

- Hospedar vários sites em um único servidor usando vários certificados SSL em um único servidor e associando cada certificado a um endereço IP específico.

- Operar aplicações de rede, como firewalls ou load balancers, que têm vários endereços IP para cada interface de rede.
- Redirecionar o tráfego interno para uma instância em espera em caso de falha na instância, atribuindo novamente o endereço IP secundário à instância em espera.

Tópicos

- [Como funcionam vários endereços IP \(p. 965\)](#)
- [Trabalhar com vários endereços IPv4 \(p. 966\)](#)
- [Trabalhar com vários endereços IPv6 \(p. 969\)](#)

Como funcionam vários endereços IP

A lista a seguir explica como vários endereços IP funcionam com interfaces de rede:

- Você pode atribuir um endereço IPv4 privado secundário a qualquer interface de rede. A interface de rede não precisa ser anexada à instância.
- Você pode atribuir vários endereços IPv6 a uma interface de rede que esteja em uma sub-rede que tem um bloco CIDR IPv6 associado.
- Você deve escolher um endereço IPv4 secundário no intervalo de bloco CIDR IPv4 da sub-rede para a interface de rede.
- Você deve escolher endereços IPv6 no intervalo de bloco CIDR IPv6 da sub-rede para a interface de rede.
- Você associa grupos de segurança a interfaces de rede, não a endereços IP individuais. Portanto, cada endereço IP especificado em uma interface de rede está sujeito ao grupo de segurança de sua interface de rede.
- Vários endereços IP podem ser atribuídos e ter a atribuição cancelada para interfaces de rede anexadas ou instâncias paradas.
- Os endereços IPv4 privados secundários que são atribuídos a uma interface de rede podem ser atribuídos novamente para outra interface de rede se você permitir isso explicitamente.
- Um endereço IPv6 não pode ser atribuído novamente a outra interface de rede. Você deve primeiro cancelar a atribuição do endereço IPv6 da interface de rede existente.
- Ao atribuir vários endereços IP a uma interface de rede usando as ferramentas da linha de comando ou a API, a operação inteira falhará se um dos endereços IP não puder ser atribuído.
- Os endereços IPv4 privados primários, os endereços IPv4 privados secundários, os endereços IP elásticos e os endereços IPv6 permanecem com a interface de rede secundária quando ela é desanexada de uma instância ou anexada a uma instância.
- Embora não seja possível desanexar a interface de rede primária de uma instância, você pode atribuir novamente o endereço IPv4 privado secundário da interface de rede primária para outra interface de rede.

A lista a seguir explica como vários endereços IP funcionam com endereços IP elásticos (IPv4 somente):

- Cada endereço IPv4 privado pode ser associado a um único endereço IP elástico e vice-versa.
- Quando um endereço IPv4 privado secundário é atribuído novamente a outra interface, o endereço IPv4 privado secundário retém a associação a um endereço IP elástico.
- Quando a atribuição de um endereço IPv4 privado secundário é cancelada em uma interface, um endereço IP elástico associado é automaticamente desassociado do endereço IPv4 privado secundário.

Trabalhar com vários endereços IPv4

Você pode atribuir um endereço IPv4 privado secundário a uma instância, associar um endereço IPv4 elástico a um endereço IPv4 privado secundário e cancelar a atribuição de um endereço IPv4 privado secundário.

Tópicos

- [Atribuir um endereço IPv4 privado secundário \(p. 966\)](#)
- [Configurar o sistema operacional na instância para reconhecer endereços IPv4 privados secundários \(p. 968\)](#)
- [Associar um endereço IP elástico ao endereço IPv4 privado secundário \(p. 968\)](#)
- [Visualizar endereços IPv4 privados secundários \(p. 968\)](#)
- [Cancelar a atribuição de um endereço IPv4 privado secundário \(p. 969\)](#)

Atribuir um endereço IPv4 privado secundário

Você pode atribuir o endereço IPv4 privado secundário à interface de rede para uma instância ao executar a instância ou após a instância estar em execução. Esta seção inclui os seguintes procedimentos.

- [Para atribuir um endereço IPv4 privado secundário ao executar uma instância \(p. 966\)](#)
- [Para atribuir um endereço IPv4 secundário durante a execução usando a linha de comando \(p. 967\)](#)
- [Para atribuir um endereço IPv4 privado secundário a uma interface de rede \(p. 967\)](#)
- [Para atribuir um IPv4 privado secundário a uma instância existente usando a linha de comando \(p. 967\)](#)

Para atribuir um endereço IPv4 privado secundário ao executar uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Launch Instance (Executar instância).
3. Selecione uma AMI, escolha um tipo de instância e escolha Next: Configure Instance Details.
4. Na página Configure Instance Details, em Network, selecione uma VPC, e em Subnet, selecione uma sub-rede.
5. Na seção Network Interfaces, faça o seguinte, e escolha Next: Add Storage:
 - Para adicionar outra interface de rede, escolha Add Device. O console permite que você especifique até duas interfaces de rede ao executar uma instância. Depois de executar a instância, escolha Network Interfaces no painel de navegação para adicionar mais interfaces de rede. O número total de interfaces de rede que você pode associar varia por tipo de instância. Para obter mais informações, consulte [Endereços IP por interface de rede por tipo de instância \(p. 1004\)](#).

Important

Quando você adiciona uma segunda interface de rede, o sistema não pode mais atribuir um endereço IPv4 público automaticamente. Você não poderá se conectar à instância via IPv4 a menos que você atribua um endereço IP elástico à interface de rede primária (eth0). Você pode atribuir um endereço IP elástico depois de concluir o assistente de execução. Para obter mais informações, consulte [Trabalhar com endereços IP elásticos \(p. 994\)](#).

- Para cada interface de rede, em Secondary IP addresses, escolha Add IP e digite um endereço IP privado no intervalo da sub-rede, ou aceite o valor padrão Auto-assign para permitir que a Amazon selecione um endereço.
6. Na próxima página Add Storage, você pode especificar volumes para anexar à instância além dos volumes especificados pela AMI (como o volume do dispositivo raiz) e, em seguida, selecione Next: Add Tags.

7. Na página Adicionar tags, especifique as tags da instância, como nome amigável, e selecione Próximo: Configurar security group.
8. Na página Configure Security Group, selecione um security group existente ou crie um novo. Escolha Review and Launch.
9. Na página Review Instance Launch, reveja as configurações, e escolha Launch para escolher um par de chaves e executar a instância. Se você for novo no Amazon EC2 e não tiver criado nenhum par de chaves, o assistente solicitará que você crie um.

Important

Depois de adicionar um endereço IP privado secundário a uma interface de rede, você deve conectar-se à instância e configurar o endereço IP privado secundário na própria instância. Para obter mais informações, consulte [Configurar o sistema operacional na instância para reconhecer endereços IPv4 privados secundários \(p. 968\)](#).

Para atribuir um endereço IPv4 secundário durante a execução usando a linha de comando

- Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).
 - A opção `--secondary-private-ip-addresses` com o comando `run-instances` (AWS CLI)
 - Defina `-NetworkInterface` e especifique o parâmetro `PrivateIpAddresses` com o comando `New-EC2Instance` (AWS Tools for Windows PowerShell).

Para atribuir um endereço IPv4 privado secundário a uma interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Network Interfaces e, em seguida, selecione a interface de rede anexada à instância.
3. Escolha Ações, Gerenciar endereços IP.
4. Em IPv4 Addresses, selecione Assign new IP.
5. Insira um endereço IPv4 específico que esteja no intervalo da sub-rede para a instância ou deixe o campo em branco para permitir que a Amazon selecione um endereço IP para você.
6. (Opcional) Escolha Allow reassignment para permitir que o endereço IP privado secundário seja atribuído novamente se ele já estiver atribuído a outra interface de rede.
7. Escolha Yes, Update.

Como alternativa, você pode atribuir um endereço IPv4 privado secundário a uma instância. Escolha Instances no painel de navegação, selecione a instância, e escolha Actions, Networking, Manage IP Addresses. Você pode configurar as mesmas informações que configurou nas etapas acima. O endereço IP é atribuído à interface de rede primária (eth0) da instância.

Para atribuir um IPv4 privado secundário a uma instância existente usando a linha de comando

- Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).
 - `assign-private-ip-addresses` (AWS CLI)
 - `Register-EC2PrivateIpAddress` (AWS Tools for Windows PowerShell)

Configurar o sistema operacional na instância para reconhecer endereços IPv4 privados secundários

Depois de atribuir um endereço IPv4 privado secundário à instância, você precisa configurar o sistema operacional na instância para reconhecer o endereço IP privado secundário.

Para obter informações sobre como configurar uma instância Windows, consulte [Configurar um endereço IPv4 privado secundário para uma instância do Windows. \(p. 610\)](#).

Associar um endereço IP elástico ao endereço IPv4 privado secundário

Para associar um endereço IP elástico a um endereço IPv4 privado secundário

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Escolha Actions e, em seguida, selecione Associate address.
4. Em Network interface, selecione a interface de rede, e selecione o endereço IP secundário na lista Private IP.
5. Escolha Associate.

Para associar um endereço IP elástico a um endereço IPv4 privado secundário usando a linha de comando

- Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).
 - `associate-address` (AWS CLI)
 - `Register-EC2Address` (AWS Tools for Windows PowerShell)

Visualizar endereços IPv4 privados secundários

Para visualizar os endereços IPv4 privados atribuídos a uma interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede com os endereços IP privados a serem exibidos.
4. Na guia Details no painel de detalhes, marque os campos Primary private IPv4 IP e Secondary private IPv4 IPs para o endereço IPv4 privado primário e qualquer endereço IPv4 privado secundário atribuído à interface de rede.

Para visualizar os endereços IPv4 privados atribuídos a uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância com os endereços IPv4 privados a serem exibidos.
4. Na guia Description no painel de detalhes, marque os campos Private IPs e Secondary private IPs para o endereço IPv4 privado primário e qualquer endereço IPv4 privado secundário atribuído à instância por meio da interface de rede.

CANCELAR A ATRIBUIÇÃO DE UM ENDEREÇO IPv4 PRIVADO SECUNDÁRIO

Se você não precisar mais de um endereço IPv4 privado secundário, poderá cancelar sua atribuição na instância ou na interface de rede. Quando a atribuição de um endereço IPv4 privado secundário é cancelada de uma interface de rede, o endereço IP elástico (se houver) também é desassociado.

Para cancelar a atribuição de um endereço IPv4 privado secundário de uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância, escolha Actions, Networking, Manage IP Addresses.
4. Em IPv4 Addresses, escolha Unassign para cancelar a atribuição do endereço IPv4.
5. Escolha Yes, Update.

Para cancelar a atribuição de um endereço IPv4 privado secundário de uma interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede, escolha Actions, Manage IP Addresses.
4. Em IPv4 Addresses, escolha Unassign para cancelar a atribuição do endereço IPv4.
5. Escolha Yes, Update.

Para cancelar a atribuição de um endereço IPv4 privado secundário usando a linha de comando

- Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).
 - `unassign-private-ip-addresses` (AWS CLI)
 - `Unregister-EC2PrivateIpAddress` (AWS Tools for Windows PowerShell)

TRABALHAR COM VÁRIOS ENDEREÇOS IPv6

Você pode atribuir vários endereços IPv6 à instância, visualizar os endereços IPv6 atribuídos à instância e cancelar a atribuição de endereços IPv6 da instância.

Tópicos

- [Atribuir vários endereços IPv6 \(p. 969\)](#)
- [Visualizar os endereços IPv6 \(p. 971\)](#)
- [Cancelar a atribuição de um endereço IPv6 \(p. 971\)](#)

Atribuir vários endereços IPv6

Você pode atribuir um ou mais endereços IPv6 à instância durante ou após a execução. Para atribuir um endereço IPv6 a uma instância, a VPC e a sub-rede em que você executa a instância devem ter um bloco CIDR IPv6 associado. Para obter mais informações, consulte [VPCs e sub-redes](#) no Guia do usuário da Amazon VPC.

Para atribuir vários endereços IPv6 durante a execução

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel, escolha Launch Instance (Executar instância).
3. Selecione uma AMI, escolha um tipo de instância e escolha Next: Configure Instance Details. Escolha um tipo de instância que seja compatível com o IPv6. Para obter mais informações, consulte [Tipos de instância \(p. 149\)](#).
4. Na página Configure Instance Details, selecione uma VPC na lista Network e uma sub-rede na lista Subnet.
5. Na seção Network Interfaces, faça o seguinte, e escolha Next: Add Storage:
 - Para atribuir um único endereço IPv6 à interface de rede primária (eth0), em IPv6 IPs, escolha Add IP. Para adicionar um endereço IPv6 secundário, selecione novamente Adicionar IP. Você pode informar um endereço IPv6 de intervalo da sub-rede ou deixar o valor padrão Autoatribuir para permitir que a Amazon escolha um endereço IPv6 da sub-rede para você.
 - Escolha Add Device para adicionar outra interface de rede e repita as etapas acima para adicionar um ou mais endereços IPv6 à interface de rede. O console permite que você especifique até duas interfaces de rede ao executar uma instância. Depois de executar a instância, escolha Network Interfaces no painel de navegação para adicionar mais interfaces de rede. O número total de interfaces de rede que você pode associar varia por tipo de instância. Para obter mais informações, consulte [Endereços IP por interface de rede por tipo de instância \(p. 1004\)](#).
6. Siga as próximas etapas do assistente para anexar volumes e marcar sua instância.
7. Na página Configure Security Group, selecione um security group existente ou crie um novo. Se desejar que a instância seja acessível por IPv6, verifique se o security group tem regras que permitem acesso de endereços IPv6. Para obter mais informações, consulte [Regras de grupo de segurança para diferentes casos de uso \(p. 1233\)](#). Escolha Review and Launch.
8. Na página Review Instance Launch, reveja as configurações, e escolha Launch para escolher um par de chaves e executar a instância. Se você for novo no Amazon EC2 e não tiver criado nenhum par de chaves, o assistente solicitará que você crie um.

Você pode usar a tela Instances do console do Amazon EC2 para atribuir vários endereços IPv6 a uma instância existente. Isso atribui os endereços IPv6 à interface de rede primária (eth0) da instância. Para atribuir um endereço IPv6 específico à instância, verifique se o endereço IPv6 já não está atribuído a outra instância ou interface de rede.

Para atribuir vários endereços IPv6 a uma instância existente

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).
4. Em IPv6 Addresses, escolha Assign new IP para cada endereço IPv6 que você deseja adicionar. Você pode especificar um endereço IPv6 no intervalo da sub-rede ou deixar o valor Auto-assign para permitir que a Amazon escolha um endereço IPv6 para você.
5. Escolha Yes, Update.

Como alternativa, você pode atribuir vários endereços IPv6 a uma interface de rede existente. A interface de rede deve ter sido criada em uma sub-rede com um bloco CIDR IPv6 associado. Para atribuir um endereço IPv6 específico à interface de rede, assegure-se de que o endereço IPv6 já não tenha sido designado para outra interface de rede.

Para atribuir vários endereços IPv6 a uma interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede, escolha Actions, Manage IP Addresses.

4. Em IPv6 Addresses, escolha Assign new IP para cada endereço IPv6 que você deseja adicionar. Você pode especificar um endereço IPv6 no intervalo da sub-rede ou deixar o valor Auto-assign para permitir que a Amazon escolha um endereço IPv6 para você.
5. Escolha Yes, Update.

Visão geral da CLI

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- Atribuir um endereço IPv6 durante a execução:
 - Use a opção `--ipv6-addresses` ou `--ipv6-address-count` com o comando [run-instances](#) (AWS CLI)
 - Defina `-NetworkInterface` e especifique os parâmetros `Ipv6Addresses` ou `Ipv6AddressCount` com o comando [New-EC2Instance](#) (AWS Tools for Windows PowerShell).
- Atribuir um endereço IPv6 a uma interface de rede:
 - [assign-ipv6-addresses](#) (AWS CLI)
 - [Register-EC2Ipv6AddressList](#) (AWS Tools for Windows PowerShell)

Visualizar os endereços IPv6

Você pode visualizar os endereços IPv6 de uma instância ou de uma interface de rede.

Para visualizar os endereços IPv6 privados atribuídos a uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione sua instância. No painel de detalhes, reveja o campo IPv6 IPs.

Para visualizar os endereços IPv6 atribuídos a uma interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede. No painel de detalhes, reveja o campo IPv6 IPs.

Visão geral da CLI

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- Visualizar endereços IPv6 de uma instância:
 - [describe-instances](#) (AWS CLI)
 - [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).
- Para visualizar os endereços IPv6 de uma interface de rede:
 - [describe-network-interfaces](#) (AWS CLI)
 - [Get-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Cancelar a atribuição de um endereço IPv6

Você pode cancelar a atribuição de um endereço IPv6 da interface de rede primária de uma instância ou cancelar a atribuição de um endereço IPv6 de uma interface de rede.

Para cancelar a atribuição de um endereço IPv6 de uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Actions (Ações), Networking (Redes), Manage IP Addresses (Gerenciar endereços IP).
4. Em IPv6 Addresses, escolha Unassign para cancelar a atribuição do endereço IPv6.
5. Escolha Yes, Update.

Para cancelar a atribuição de um endereço IPv6 de uma interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede, escolha Actions, Manage IP Addresses.
4. Em IPv6 Addresses, escolha Unassign para cancelar a atribuição do endereço IPv6.
5. Escolha Save (Salvar).

Visão geral da CLI

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [unassign-ipv6-addresses](#) (AWS CLI)
- [Unregister-EC2Ipv6AddressList](#) (AWS Tools for Windows PowerShell).

Traga seus próprios endereços IP (BYOIP) no Amazon EC2

Você pode trazer parte ou todo o seu intervalo de endereços IPv4 ou IPv6 publicamente roteáveis da rede on-premises para sua conta da AWS. Você continua a ter o intervalo de endereços, mas a AWS o anuncia na Internet por padrão. Depois de levar o intervalo de endereços para a AWS, ele aparece em sua conta da AWS como um grupo de endereços.

O BYOIP não está disponível em todas as regiões e para todos os recursos. Para obter uma lista das regiões e recursos compatíveis, consulte [Perguntas frequentes sobre Traga seu próprio IP](#).

Note

As etapas a seguir descrevem como trazer seu próprio intervalo de endereços IP para uso somente no Amazon EC2. Para obter as etapas para trazer seu próprio intervalo de endereços IP para uso no AWS Global Accelerator, consulte [Traga seus próprios endereços IP \(BYOIP\) no AWS Global Accelerator Developer Guide](#) (Guia do desenvolvedor do AWS Global Accelerator).

Tópicos

- [Requisitos e cotas \(p. 973\)](#)
- [Configurar seu intervalo de endereços BYOIP \(p. 973\)](#)
- [Trabalhar com o intervalo de endereços \(p. 980\)](#)
- [Saiba mais \(p. 981\)](#)

Requisitos e cotas

- O intervalo de endereços deve ser registrado com o registro de Internet regional (RIR - regional internet registry), como o American Registry for Internet Numbers (ARIN) ou o Réseaux IP Européens Network Coordination Centre (RIPE) ou o Asia-Pacific Network Information Centre (APNIC). Ele deve ser registrado para uma entidade empresarial ou institucional e não pode ser registrado para uma única pessoa.
- O intervalo de endereços IPv4 mais específico que você pode trazer é /24.
- O intervalo de endereços IPv6 mais específico que você pode trazer é /48 para CIDRs anunciados publicamente e /56 para CIDRs que [não são anunciados publicamente \(p. 979\)](#).
- Você pode levar cada intervalo de endereços para uma região de cada vez.
- É possível levar um total de cinco intervalos de endereços IPv4 e IPv6 por região para sua conta da AWS.
- Você não pode compartilhar seu intervalo de endereços IP com outras contas usando AWS Resource Access Manager (AWS RAM).
- Os endereços no intervalo de endereços IP devem ter um histórico limpo. Podemos investigar a reputação do intervalo de endereços IP e reservar o direito de rejeitar um intervalo de endereços IP, se ele contiver um endereço IP que tenha má reputação ou esteja associado a comportamento mal-intencionado.
- É necessário possuir o endereço IP usado. Isso significa que somente os seguintes são compatíveis:
 - ARIN — os tipos de rede "Alocação direta" e "Atribuição direta"
 - Status de alocação RIPE - "ALLOCATED PA", "LEGACY", "ASSIGNED PI", e "ALLOCATED-BY-RIR"
 - APNIC – os status de alocação "ALLOCATED PORTABLE" e "ASSIGNED PORTABLE"

Configurar seu intervalo de endereços BYOIP

O processo para configurar o BYOIP tem estas fases:

- Preparação

Para fins de autenticação, crie um par de chaves RSA e use-o para gerar um certificado X.509 autoassinado.

- Configuração do RIR

Registre-se na Infraestrutura de Chave Pública de Recursos (RPKI – Resource Public Key Infrastructure) do seu RIR e registre uma Route Origin Authorization (ROA – Autorização de Origem de Rota) que define o intervalo de endereços desejado, os Autonomous System Numbers (ASNs – Números de sistema autônomo) autorizados a anunciar o intervalo de endereços e uma data de expiração. Faça upload do certificado autoassinado nos comentários do registro RDAP.

- Configuração do Amazon

Assine uma mensagem de contexto de autorização CIDR com a chave RSA privada que você criou e faça upload da mensagem e da assinatura para a Amazon usando a AWS Command Line Interface.

Para trazer vários intervalos de endereços, você deve repetir esse processo com cada intervalo de endereços. Colocar em um intervalo de endereços não tem efeito em quaisquer intervalos de endereços que você trouxe anteriormente.

Execute as tarefas a seguir para configurar o acesso ao . Para algumas tarefas, você executa comandos do Linux. No Windows, é possível usar o [Subsistema Windows para Linux](#) a fim de executar comandos do Linux.

Tarefas

- [Criar um par de chaves e um certificado \(p. 974\)](#)
- [Criar um objeto ROA em seu RIR \(p. 977\)](#)
- [Atualizar o registro RDAP em seu RIR \(p. 977\)](#)
- [Provisionar o intervalo de endereços em AWS \(p. 978\)](#)
- [Anunciar o intervalo de endereços por meio da AWS \(p. 979\)](#)
- [Desprovisionar o intervalo de endereços \(p. 980\)](#)

Criar um par de chaves e um certificado

Siga o procedimento a seguir para criar um certificado autoassinado X.509 e adicione-o ao registro RDAP para seu RIR. Os comandos openssl requerem o OpenSSL versão 1.0.2 ou posterior.

Copie os comandos abaixo e substitua apenas os valores de espaço reservado (em texto itálico colorido).

Para criar um certificado autoassinado X.509 e adicioná-lo ao registro RDAP

Este procedimento segue a prática recomendada de criptografar sua chave RSA privada e exigir uma senha para acessá-la.

1. Gere um par de chaves RSA de 2048 bits como mostrado a seguir.

```
$ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out private-key.pem
```

O parâmetro `-aes256` especifica o algoritmo usado para criptografar a chave privada. O comando retorna a seguinte saída, incluindo prompts para definir uma frase de acesso:

```
.....+++
.+++
Enter PEM pass phrase: xxxxxxxx
Verifying - Enter PEM pass phrase: xxxxxxxx
```

Você pode fazer inspecionar a chave pública com o seguinte comando:

```
$ openssl pkey -in private-key.pem -text
```

Isso retorna um prompt de frase-senha e o conteúdo da chave, que deve ser semelhante ao seguinte:

```
Enter pass phrase for private-key.pem: xxxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seicioizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAriwmSd/8TDvHJMY9FvAlvWuTsv5l0tJKk+a91K4+t03UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRs01AhJ
DnPZPneweboo+K3Q31wbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAECggEACiJUj2hfJkV47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fxt0SPUNbhUxbBNbshoJGuffwXPli1SXnpzvkdU4Hyco4zgbhXFse
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNr1H0jDhpioL8cQEBdBJyVF5X0wymEbmv
mC0jgH/MxsBAPWW6ZKicg9ULM1WiAZ3MRAZPjHHgpYKAAsUWKAbCBwVQcVjGO59W
jfZjzTX5p0tVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63f1wLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvmwUj4VSWOHZBHLv4evJaaia0uQjIoi1UDA8AYitqhqX1NmCcbehGH8yuXj/
```

```
v6V3CzMKDkmRr1Nr0NnSz5QsndQ04Z6ihAQ1PmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5y0IC1Pz2T85g0e1i8kwZws+xlpG6uBT6lMIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzYZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TV1YaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nPp/JyRwgjOrN1jk7DHes+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3azZX/Bdh9woTXqhXDrrSwWIInVYMQPypk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtxlWtheKRYkQmzQZXbwDIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
```

```

31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
38:eb:2e:96:87:35:9f:cc:5d
exponent1:
00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
06:57:6d:67:48:85:8c:88:dd
coefficient:
3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
9a:77:5a:e5:87:d5:4f:01

```

Mantenha sua chave privada em um local seguro quando ela não estiver em uso.

2. Gere sua chave pública a partir da chave privada da seguinte forma. Você usará isso mais tarde para testar se a mensagem de autorização assinada valida corretamente.

```
$ openssl rsa -in private-key.pem -pubout > public-key.pem
```

Na inspeção, sua chave pública deve ter um aspecto semelhante a este:

```

$ cat public-key.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAxQVx0SOB1SgIYd7HonIq
KIswkU2yXtfmLMTU42u8isqrViBVgxowB0OBQh5Tzjk1Sfjaj++MPeqD0wz0t8a
PZGkMmQRZ9mBKdhAAub3990YhzUZmWVJpJ9MxzkhKTZmNnzMSEgcXsJcURQJ4sJk
nf/Ew7xyTGPRbwCL1rk7L+ZdLSSpPmvdSuPrTt1HQoe0p6OVlxMX7Aa1t4NcnaN0
wbMfIuf2I1TnDQKcu4HtvxYsgN2glyQeq+p7heh/JkYCOK+L5DEbDpQISQ52TzXs
Hm6KPit0N5cG4G5jig/8/bL5PDF/oVEwbsF9H0bWxvjyyMN8VkrxqzEp9gc7D1bg
ywIDAQAB
-----END PUBLIC KEY-----

```

3. Gere um certificado X.509 usando o par de chaves criado no anterior. Neste exemplo, o certificado expira em 365 dias, após o qual ele não é mais confiável. Defina a expiração adequadamente. O comando `tr -d "\n"` remove caracteres de nova linha (quebras de linha) da saída. Você precisa fornecer um nome comum quando solicitado, mas os outros campos podem ser deixados em branco.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" > certificate.pem
```

Isso resulta em uma saída semelhante à seguinte:

```
Enter pass phrase for private-key.pem: XXXXXXXX
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

Você pode inspecionar o certificado usando o seguinte comando:

```
$ cat certificate.pem
```

A saída deve ser uma string longa, codificada em PEM, sem quebras de linha, prefaciada por -----BEGIN CERTIFICATE----- e seguida por -----END CERTIFICATE-----.

Criar um objeto ROA em seu RIR

Crie um objeto ROA para autorizar os Amazon ASNs 16509 e 14618 a anunciar seu intervalo de endereços, bem como dos ASNs atualmente autorizados a anunciar o intervalo de endereços. Você deve definir o tamanho máximo como o menor prefixo que deseja levar (por exemplo, /24). Pode demorar até 24 horas para que a ROA se torne disponível para a Amazon. Para obter mais informações, consulte o seu RIR:

- ARIN — [Solicitações de ROA](#)
- RIPE — [Gerenciamento de ROAs](#)
- APNIC — [Gerenciamento de rotas](#)

Atualizar o registro RDAP em seu RIR

Adicione o certificado criado anteriormente ao registro RDAP do RIR. Certifique-se de incluir as strings -----BEGIN CERTIFICATE----- e -----END CERTIFICATE----- antes e depois da parte codificada. Todo esse conteúdo deve estar em uma única e longa linha. O procedimento para atualizar o RDAP depende do RIR:

- No ARIN, inclua o certificado na seção "Public Comments (Comentários públicos) do intervalo de endereços. Não o adicione à seção de comentários da sua organização.
- No RIPE, inclua o certificado como um novo campo "descr" para o intervalo de endereços. Não o adicione à seção de comentários da sua organização.
- Para o APNIC, envie a chave pública por e-mail para helpdesk@apnic.net para adicioná-la manualmente ao campo "observações" do seu intervalo de endereços. Envie o e-mail usando o contato autorizado do APNIC para os endereços IP.

Provisionar o intervalo de endereços em AWS

Ao provisionar um intervalo de endereços para uso com a AWS, você está confirmando que é o proprietário do intervalo de endereços e autoriza a Amazon a anunciar-lo. Também verificamos se você possui o intervalo por meio de uma mensagem de autorização assinada. Essa mensagem é assinada com o par de chaves X.509 autoassinadas que você usou ao atualizar o registro RDAP com o certificado X.509. A AWS requer uma mensagem de autorização assinada criptograficamente que apresenta ao RIR. O RIR autentica a assinatura em relação ao certificado que você adicionou ao RDAP e verifica os detalhes da autorização em relação ao ROA.

Para provisionar o intervalo de endereços

1. Compose message

Componha a mensagem de autorização de texto simples. O formato da mensagem é o seguinte, em que a data é a data de expiração da mensagem:

```
1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
```

Substitua o número da conta, o intervalo de endereços e a data de expiração por seus próprios valores para criar uma mensagem semelhante à seguinte:

```
1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS
```

Isso não deve ser confundido com uma mensagem ROA, que tem uma aparência semelhante.

2. Assinar mensagens

Assine a mensagem de texto sem formatação usando a chave privada criada anteriormente. A assinatura retornada pelo comando é uma string longa que você precisará copiar para uso na próxima etapa.

Important

Recomendamos que você copie e cole esse comando. Com exceção do conteúdo da mensagem, não modifique nem substitua nenhum dos valores.

```
$ echo -n "1|aws|123456789012|198.51.100.0/24|20211231|SHA256|RSAPSS" | openssl dgst -sha256 -sigopt rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM | openssl base64 | tr -- '+=' '-'_-' | tr -d "\n"
```

3. Endereço de provisão

Use o comando [provisiona-byoip-cidr](#) da AWS CLI para provisionar o intervalo de endereços. A opção `--cidr-authorization-context` usa as strings de mensagem e assinatura que você criou anteriormente.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context  
Message="message",Signature="signature"
```

O provisionamento de um intervalo de endereços é uma operação assíncrona, de modo que a chamada retorna imediatamente, mas o intervalo de endereços não está pronto para uso até que seu status mude de `pending-provision` para `provisioned`.

4. Monitorar o andamento

Pode levar até três semanas para concluir o processo de provisionamento para intervalos que permitem anúncios públicos. Use o comando [describe-byoi-p-cidrs](#) para monitorar seu progresso, como neste exemplo:

```
aws ec2 describe-byoi-p-cidrs --max-results 5
```

Se houver problemas durante o provisionamento e o status for para `failed-provision`, o comando `provision-byoi-p-cidr` deverá ser executado novamente após os problemas terem sido resolvidos.

Provisionar um intervalo de endereços IPv6 que não seja anunciado publicamente

Por padrão, um intervalo de endereços é provisionado para ser publicamente anunciado na Internet. É possível provisionar um intervalo de endereços IPv6 que não será anunciado publicamente. Para rotas que não permitem anúncios públicos, o processo de provisionamento geralmente é concluído em minutos. Quando você associa um bloco CIDR IPv6 de um intervalo de endereços não públicos com uma VPC, o CIDR IPv6 só pode ser acessado por uma conexão do AWS Direct Connect.

Não é necessário um ROA para provisionar um intervalo de endereços não públicos.

Important

Você só pode especificar se um intervalo de endereços é anunciado publicamente durante o provisionamento. Não é possível alterar o status de anúncio de um intervalo de endereços posteriormente.

Para provisionar um intervalo de endereços IPv6 que não será anunciado publicamente, use o seguinte comando [provision-byoi-p-cidr](#).

```
aws ec2 provision-byoi-p-cidr --cidr address-range --cidr-authorization-context  
Message="$text_message",Signature="$signed_message" --no-publicly-advertisible
```

Anunciar o intervalo de endereços por meio da AWS

Após ser provisionado, o intervalo de endereços estará pronto para ser anunciado. É necessário anunciar o intervalo de endereço exato que você provisionou. Não é possível anunciar apenas uma parte do intervalo de endereço provisionado.

Se você provisionou um intervalo de endereços IPv6 que não será anunciado publicamente, não será necessário concluir esta etapa.

Recomendamos interromper o anúncio do intervalo de endereços em outros locais antes de anunciar por meio da AWS. Se você mantiver o anúncio de seu intervalo de endereços IP em outros locais, não poderemos oferecer suporte a ele ou solucionar problemas de forma confiável. Especificamente, não podemos garantir que o tráfego para o intervalo de endereços entre em nossa rede.

Para minimizar o tempo de inatividade, você pode configurar os recursos da AWS para usar um endereço do grupo de endereços antes de ele ser anunciado e, em seguida, interromper simultaneamente o anúncio no local atual e iniciar o anúncio por meio da AWS. Para obter mais informações sobre a alocação de um endereço IP elástico em seu grupo de endereços, consulte [Alocar um endereço IP elástico \(p. 994\)](#).

Limitations

- Você pode executar o comando `advertise-byoi-p-cidr` no máximo uma vez a cada 10 segundos, mesmo que você especifique diferentes intervalos de endereços de cada vez.

- Você pode executar o comando `withdraw-byoip-cidr` no máximo uma vez a cada 10 segundos, mesmo que você especifique diferentes intervalos de endereços de cada vez.

Para anunciar o intervalo de endereços, use o seguinte comando `advertise-byoip-cidr`.

```
aws ec2 advertise-byoip-cidr --cidr address-range
```

Para interromper o anúncio do intervalo de endereços, use o seguinte comando `withdraw-byoip-cidr`.

```
aws ec2 withdraw-byoip-cidr --cidr address-range
```

Desprovisionar o intervalo de endereços

Para interromper o uso do intervalo de endereços com a AWS, primeiro libere todos os endereços IP elásticos e desassocie todos os blocos CIDR IPv6 que ainda estiverem alocados do grupo de endereços. Depois, pare de anunciar o intervalo de endereços e, por fim, desprovisione o intervalo de endereços.

Não é possível desprovisionar uma parte do intervalo de endereços. Se você quiser usar um intervalo de endereços mais específico com a AWS, cancele o provisionamento de todo o intervalo de endereços e provisão um intervalo de endereços mais específico.

(IPv4) Para liberar cada endereço IP elástico, use o seguinte comando `release-address`.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcbabc
```

(IPv6) Para desassociar um bloco CIDR IPv6, use o seguinte comando `disassociate-vpc-cidr-block`.

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
```

Para interromper o anúncio do intervalo de endereços, use o seguinte comando `withdraw-byoip-cidr`.

```
aws ec2 withdraw-byoip-cidr --cidr address-range
```

Para desprovisionar o intervalo de endereços, use o seguinte comando `deprovision-byoip-cidr`.

```
aws ec2 deprovision-byoip-cidr --cidr address-range
```

Pode levar até um dia para desprovisionar um intervalo de endereços.

Trabalhar com o intervalo de endereços

É possível visualizar e trabalhar com os intervalos de endereços IPv4 e IPv6 que você provisionou na conta.

Intervalos de endereços IPv4

É possível criar um endereço IP elástico pelo grupo de endereços IPv4 e usá-lo com os recursos da AWS, como instâncias do EC2, gateways NAT e平衡adores de carga de rede.

Para visualizar informações sobre os grupos de endereços IPv4 que você provisionou na conta, use o seguinte comando `describe-public-ipv4-pools`.

```
aws ec2 describe-public-ipv4-pools
```

Para criar um endereço IP elástico pelo grupo de endereços IPv4, use o comando [allocate-address](#). É possível usar a opção `--public-ipv4-pool` para especificar o ID do grupo de endereços retornado por `describe-byoip-cidrs`. Ou usar a opção `--address` para especificar um endereço do intervalo de endereços que você provisionou.

Intervalos de endereços IPv6

Para visualizar informações sobre os grupos de endereços IPv6 que você provisionou na conta, use o seguinte comando [describe-ipv6-pools](#).

```
aws ec2 describe-ipv6-pools
```

Para criar uma VPC e especificar um CIDR IPv6 pelo grupo de endereços IPv6, use o seguinte comando [create-vpc](#). Para permitir que a Amazon escolha o CIDR IPv6 do grupo de endereços IPv6, omita a opção `--ipv6-cidr-block`.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-pool pool-id
```

Para associar um bloco CIDR IPv6 do grupo de endereços IPv6 a uma VPC, use o seguinte comando [associate-vpc-cidr-block](#). Para permitir que a Amazon escolha o CIDR IPv6 do grupo de endereços IPv6, omita a opção `--ipv6-cidr-block`.

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-cidr --ipv6-pool pool-id
```

Para visualizar as VPCs e as informações do grupo de endereços IPv6 associado, use o comando [describe-vpcs](#). Para visualizar informações sobre blocos CIDR IPv6 associados de um grupo de endereços IPv6 específico, use o seguinte comando [get-associated-ipv6-pool-cidrs](#).

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id
```

Se você desassociar o bloco CIDR IPv6 da VPC, ele será liberado de volta para o grupo de endereços IPv6.

Para obter mais informações sobre como trabalhar com blocos CIDR IPv6 no console da VPC, consulte [Trabalhar com VPCs e sub-redes](#) no Guia do usuário da Amazon VPC.

Saiba mais

Para obter mais informações, consulte o [.AWSConversa técnica onlineMergulho profundo em Traga seu próprio IP](#).

Atribuição de prefixos a interfaces de rede do Amazon EC2

Você pode atribuir um intervalo de CIDR IPv4 ou IPv6 privado, automático ou manualmente, às suas interfaces de rede. Ao atribuir prefixos, você dimensiona e simplifica o gerenciamento de aplicações, incluindo aplicações de contêiner e rede que exigem vários endereços IP em uma instância.

As seguintes opções estão disponíveis:

- Atribuição automática—AWS escolhe o prefixo do IPv4 ou IPv6 CIDR da sua sub-rede VPC e atribui à sua interface de rede.

- Atribuição manual— Você especifica o prefixo dos CIDRs IPv4 e IPv6 da sub-rede da VPC, e AWS verifica se o prefixo ainda não está atribuído a outros recursos antes de atribuí-lo à interface de rede.

Atribuir prefixos apresenta os seguintes benefícios:

- Endereços IP aumentados em uma interface de rede — Quando você usa um prefixo, atribui um bloco de endereços IP em vez de endereços IP individuais. Isso aumenta o número de endereços IP em uma interface de rede.
- Gerenciamento simplificado da VPC para contêineres — em aplicações de contêiner, cada contêiner requer um endereço IP exclusivo. A atribuição de prefixos à instância simplifica o gerenciamento de suas VPCs, pois você pode iniciar e encerrar contêineres sem precisar chamar APIs do Amazon EC2 para atribuições de IP individuais.

Tópicos

- [Noções básicas para atribuição de prefixos \(p. 982\)](#)
- [Considerações e limites para prefixos \(p. 982\)](#)
- [Trabalhar com prefixos \(p. 983\)](#)

Noções básicas para atribuição de prefixos

- Você pode atribuir um prefixo a interfaces de rede novas ou existentes.
- Para usar prefixos, primeiro atribua um prefixo à interface de rede, depois anexa a interface de rede à instância e, em seguida, configure o sistema operacional.
- Quando você escolhe a opção para especificar um prefixo, o prefixo deve atender aos seguintes requisitos:
 - O prefixo IPv4 que você pode especificar é /28.
 - O prefixo IPv6 que você pode especificar é /80.
 - O prefixo está na sub-rede CIDR da interface de rede e não se sobrepõe a outros prefixos ou endereços IP atribuídos a recursos existentes na sub-rede.
- Você pode atribuir um prefixo à interface de rede primária ou secundária.
- Você pode atribuir um endereço IP elástico a uma interface de rede que tenha um prefixo atribuído a ela.
- Um nome de host DNS privado (interno) é resolvido para o endereço IPv4 privado da instância.
- Atribuímos cada endereço IPv4 privado em uma interface de rede, incluindo aqueles de prefixos, com os seguintes formulários:
 - us-east-1Região da

`ip-private-ipv4-address.ec2.internal`

- Todas as outras regiões

`ip-private-ipv4-address.region.compute.internal`

Considerações e limites para prefixos

Leve o seguinte em consideração ao usar endpoints do :

- Interfaces de rede com prefixos são suportadas com instâncias baseadas em nitrogênio.

- Os prefixos para interfaces de rede são limitados a endereços IPv4 e IPv6 privados.
- Para ver limitações, consulte [Endereços IP por interface de rede por tipo de instância \(p. 1004\)](#).
- O número de prefixos e endereços IP em uma interface de rede deve ser menor que o limite na instância à qual a interface de rede está associada. Por exemplo, se tiver umc5.1largeinstância, o limite é 10 Endereços IPv4 e 10 Endereços IPv6 em uma interface de rede e o número total de /28 e /80 prefixos devem ser menores que 10.
- Os prefixos são incluídos nas verificações de origem/destino.

Trabalhar com prefixos

Tópicos

- [Atribuir prefixos durante a criação da interface de rede \(p. 983\)](#)
- [Atribuir prefixos a interfaces de rede existentes \(p. 988\)](#)
- [Configure seu sistema operacional para interfaces de rede com prefixos \(p. 990\)](#)
- [Exibir os prefixos atribuídos às suas interfaces de rede \(p. 990\)](#)
- [Remover prefixos de suas interfaces de rede \(p. 992\)](#)

Atribuir prefixos durante a criação da interface de rede

Se você usar a opção de atribuição automática, poderá reservar um bloco de endereços IP na sua sub-rede. AWS escolhe os prefixos deste bloco. Para obter mais informações, consulte [Comportamento do endereçamento IP para sua sub-rede](#) no Guia do usuário da Amazon VPC.

Depois de criar a interface de rede, use o comando `attach-network-interface` AWS CLI para anexar a interface de rede à sua instância. Configure seu sistema operacional para trabalhar com interfaces de rede com prefixos. Para obter mais informações, consulte [Configure seu sistema operacional para interfaces de rede com prefixos \(p. 990\)](#).

Tópicos

- [Atribuir prefixos automáticos durante a criação da interface de rede \(p. 983\)](#)
- [Atribuir prefixos específicos durante a criação da interface de rede \(p. 985\)](#)

Atribuir prefixos automáticos durante a criação da interface de rede

É possível atribuir prefixos automáticos durante a criação da interface de rede usando um dos métodos a seguir.

Console

Para atribuir prefixos automáticos durante a criação da interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Interfaces de rede e, em seguida, selecione Criar interface de rede.
3. Especifique uma descrição para a interface de rede, selecione a sub-rede na qual deseja criar a interface de rede e configure os endereços IPv4 e IPv6 privados.
4. Amplie as Configurações avançadas e faça o seguinte:
 - a. Para atribuir automaticamente um prefixo IPv4, para Delegação de prefixo IPv4, escolha Atribuir automaticamente. Em seguida, para Número de prefixos IPv4, especifique o número de prefixos a serem atribuídos.

- b. Para atribuir automaticamente um prefixo IPv6, para Delegação de prefixo IPv6, escolha Atribuir automaticamente. Em seguida, para Número de prefixos IPv6, especifique o número de prefixos a serem atribuídos.

Note

Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

5. Selecione os grupos de segurança a serem associados à interface de rede e atribua marcações de recursos, se necessário.
6. Clique em Create network interface (Criar interface de rede).

AWS CLI

Para atribuir prefixos IPv4 automáticos durante a criação da interface de rede

Usar [aws ec2 create-network-interface](#) Comando e set --ipv4-prefix-count para o número de prefixos que você deseja AWS atribuir. No exemplo a seguir, o AWS atribui 1 prefixo.

```
C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv4 automatic example" \
--ipv4-prefix-count 1
```

Exemplo de saída

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv4 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:98:65:dd:18:47",
        "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.62",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.62"
            }
        ],
        "Ipv4Prefixes": [
            {
                "Ipv4Prefix": "10.0.0.208/28"
            }
        ],
        "RequesterId": "AIDAI5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

}

Para atribuir prefixos IPv6 automáticos durante a criação da interface de rede

Usar o comando `aws ec2 create-network-interface` e sete `--ipv6-prefix-count` para o número de prefixos que você deseja atribuir. No exemplo a seguir, o AWS atribui 1 prefixo.

```
C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv6 automatic example" \
--ipv6-prefix-count 1
```

Exemplo de saída

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv6 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:bb:e4:31:fe:09",
        "NetworkInterfaceId": "eni-006edbcbfa4EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.73",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv6Prefixes": [
            {
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

Atribuir prefixos específicos durante a criação da interface de rede

É possível atribuir prefixos específicos durante a criação da interface de rede usando um dos métodos a seguir.

Console

Para atribuir prefixos específicos durante a criação da interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha Interfaces de rede e, em seguida, selecione Criar interface de rede.
3. Especifique uma descrição para a interface de rede, selecione a sub-rede na qual deseja criar a interface de rede e configure os endereços IPv4 e IPv6 privados.
4. Amplie as Configurações avançadas e faça o seguinte:
 - a. Para atribuir um prefixo IPv4 específico, para Delegação de prefixo IPv4, escolha Personalizado. Em seguida, escolha Adicionar novo e insira o prefixo a ser usado.
 - b. Para atribuir um prefixo IPv6 específico, para Delegação de prefixo IPv6, escolha Personalizado. Em seguida, escolha Adicionar novo e insira o prefixo a ser usado.

Note

Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

5. Selecione os grupos de segurança a serem associados à interface de rede e atribua marcações de recursos, se necessário.
6. Clique em Create network interface (Criar interface de rede).

AWS CLI

Para atribuir prefixos IPv4 específicos durante a criação da interface de rede

Usar `aws ec2 create-network-interface` Comando e set `--ipv4-prefixes` para os prefixos. AWS seleciona endereços IP deste intervalo. No exemplo a seguir, o prefixo CIDR é 10.0.0.0/28.

```
C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Exemplo de saída

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv4 manual example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:98:65:dd:18:47",
        "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.62",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.62"
            }
        ],
        "Ipv4Prefixes": [
            {
                "Ipv4Prefix": "10.0.0.208/28"
            }
        ]
    }
}
```

```
        },
        "RequesterId": "AIDAI5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

Para atribuir prefixos IPv6 específicos durante a criação da interface de rede

Usar o comando `aws ec2 create-network-interface` e o parâmetro `--ipv6-prefixes` para os prefixos. A AWS seleciona endereços IP deste intervalo. No exemplo a seguir, o prefixo CIDR é `2600:1f13:fc2:a700:1768::/80`.

```
C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv6 manual example" \
--ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

Exemplo de saída

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv6 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:bb:e4:31:fe:09",
        "NetworkInterfaceId": "eni-006edbca4EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.73",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv6Prefixes": [
            {
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
        ],
        "RequesterId": "AIDAI5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

Atribuir prefixos a interfaces de rede existentes

Depois de atribuir os prefixos, use o comando AWS CLI [attach-network-interface](#) para anexar a interface de rede à sua instância. Configure seu sistema operacional para trabalhar com interfaces de rede com prefixos. Para obter mais informações, consulte [Configure seu sistema operacional para interfaces de rede com prefixos \(p. 990\)](#).

Atribuir prefixos automáticos a uma interface de rede existente

É possível atribuir prefixos automáticos a uma interface de rede existente usando um dos métodos a seguir.

Console

Para atribuir prefixos automáticos a uma interface de rede existente

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede à qual atribuir os prefixos e escolha Ações, Gerenciar prefixos.
4. Para atribuir automaticamente um prefixo IPv4, para Delegação de prefixo IPv4, escolha Atribuir automaticamente. Em seguida, para Número de prefixos IPv4, especifique o número de prefixos a serem atribuídos.
5. Para atribuir automaticamente um prefixo IPv6, para Delegação de prefixo IPv6, escolha Atribuir automaticamente. Em seguida, para Número de prefixos IPv6, especifique o número de prefixos a serem atribuídos.

Note

Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

6. Escolha Save (Salvar).

AWS CLI

Você pode usar [oassign-ipv6-addresses](#) para atribuir prefixos IPv6 e o comando [assign-private-ip-addresses](#) para atribuir prefixos IPv4 a interfaces de rede existentes.

Para atribuir prefixos IPv4 automáticos a uma interface de rede existente

Usar [aassign-private-ip-addresses](#) Comando e set--ipv4-prefix-count para o número de prefixos que você deseja AWS atribuir. No exemplo a seguir, o AWS atribui 1 Prefixo IPv4.

```
C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefix-count 1
```

Exemplo de saída

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
            "Ipv4Prefix": "10.0.0.176/28"
        }
    ]
}
```

Para atribuir prefixos IPv6 automáticos a uma interface de rede existente

Usar o comando `aws ec2 assign-ipv6-addresses` e sete `--ipv6-prefix-count` para o número de prefixos que você deseja atribuir. No exemplo a seguir, o AWS atribui 1 Prefixo IPv6.

```
C:\> aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix-count 1
```

Exemplo de saída

```
{
    "AssignedIpv6Prefixes": [
        "2600:1f13:fc2:a700:18bb::/80"
    ],
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE"
}
```

Atribuir prefixos específicos a uma interface de rede existente

É possível atribuir prefixos específicos a uma interface de rede existente usando um dos métodos a seguir.

Console

Para atribuir prefixos específicos a uma interface de rede existente

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede à qual atribuir os prefixos e escolha Ações, Gerenciar prefixos.
4. Para atribuir um prefixo IPv4 específico, para Delegação de prefixo IPv4, escolha Personalizado. Em seguida, escolha Adicionar novo e insira o prefixo a ser usado.
5. Para atribuir um prefixo IPv6 específico, para Delegação de prefixo IPv6, escolha Personalizado. Em seguida, escolha Adicionar novo e insira o prefixo a ser usado.

Note

Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

6. Escolha Save (Salvar).

AWS CLI

Atribuir prefixos IPv4 específicos a uma interface de rede existente

Usar o comando `aws ec2 assign-private-ip-addresses` e sete `--ipv4-prefixes` para o prefixo. O AWS seleciona endereços IPv4 deste intervalo. No exemplo a seguir, o prefixo CIDR é 10.0.0.208/28.

```
C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.208/28
```

Exemplo de saída

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
```

```
{  
    "Ipv4Prefix": "10.0.0.208/28"  
}  
]  
}
```

Atribuir prefixos IPv6 específicos a uma interface de rede existente

Usar o comando `aws ec2 assign-ipv6-addresses` e o parâmetro `--ipv6-prefixes` para o prefixo. A AWS seleciona endereços IPv6 deste intervalo. No exemplo a seguir, o prefixo CIDR é `2600:1f13:fc2:a700:18bb::/80`.

```
C:\> aws ec2 assign-ipv6-addresses \  
--network-interface-id eni-00d577338cEXAMPLE \  
--ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

Exemplo de saída

```
{  
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE",  
    "AssignedIpv6Prefixes": [  
        {  
            "Ipv6Prefix": "2600:1f13:fc2:a700:18bb::/80"  
        }  
    ]  
}
```

Configure seu sistema operacional para interfaces de rede com prefixos

As AMIs do Amazon Linux poderão conter outros scripts instalados pela AWS, conhecidos como `ec2-net-utils`. Esses scripts opcionalmente automatizam a configuração das suas interfaces de rede. Esses scripts estão disponíveis somente para Amazon Linux.

Se você não estiver usando o Amazon Linux, poderá usar uma CNI (Container Network Interface) para o plug-in Kubernetes, ou docker se você usar o Docker para gerenciar seus contêineres.

Exibir os prefixos atribuídos às suas interfaces de rede

É possível visualizar os prefixos atribuídos às interfaces de rede usando um dos métodos a seguir.

Console

Para visualizar os prefixos automáticos a uma interface de rede existente

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede para a qual os prefixos serão visualizados e escolha a guia Detalhes.
4. O campo Delegação de prefixo IPv4 lista os prefixos IPv4 atribuídos, e o campo Delegação de prefixo IPv6 lista os prefixos IPv6 atribuídos.

AWS CLI

Você pode usar o comando `aws ec2 describe-network-interfaces` para exibir os prefixos atribuídos às interfaces de rede.

```
C:\> aws ec2 describe-network-interfaces
```

Exemplo de saída

```
{  
    "NetworkInterfaces": [  
        {  
            "AvailabilityZone": "us-west-2a",  
            "Description": "IPv4 automatic example",  
            "Groups": [  
                {  
                    "GroupName": "default",  
                    "GroupId": "sg-044c2de2c4EXAMPLE"  
                }  
            ],  
            "InterfaceType": "interface",  
            "Ipv6Addresses": [],  
            "MacAddress": "02:98:65:dd:18:47",  
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",  
            "OwnerId": "123456789012",  
            "PrivateIpAddress": "10.0.0.62",  
            "PrivateIpAddresses": [  
                {  
                    "Primary": true,  
                    "PrivateIpAddress": "10.0.0.62"  
                }  
            ],  
            "Ipv4Prefixes": [  
                {  
                    "Ipv4Prefix": "10.0.0.208/28"  
                }  
            ],  
            "Ipv6Prefixes": [],  
            "RequesterId": "AIDAI5AJI5LXF5XXDPCO",  
            "RequesterManaged": false,  
            "SourceDestCheck": true,  
            "Status": "available",  
            "SubnetId": "subnet-05eef9fb78EXAMPLE",  
            "TagSet": [],  
            "VpcId": "vpc-0e12f52b2146bf252"  
        },  
        {  
            "AvailabilityZone": "us-west-2a",  
            "Description": "IPv6 automatic example",  
            "Groups": [  
                {  
                    "GroupName": "default",  
                    "GroupId": "sg-044c2de2c411c91b5"  
                }  
            ],  
            "InterfaceType": "interface",  
            "Ipv6Addresses": [],  
            "MacAddress": "02:bb:e4:31:fe:09",  
            "NetworkInterfaceId": "eni-006edbcbfa4EXAMPLE",  
            "OwnerId": "123456789012",  
            "PrivateIpAddress": "10.0.0.73",  
            "PrivateIpAddresses": [  
                {  
                    "Primary": true,  
                    "PrivateIpAddress": "10.0.0.73"  
                }  
            ],  
            "Ipv4Prefixes": [],  
            "Ipv6Prefixes": [  
        }
```

```
{  
    "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"  
}  
,  
"RequesterId": "AIDAI5AJI5LXF5XXDPCO",  
"RequesterManaged": false,  
"SourceDestCheck": true,  
"Status": "available",  
"SubnetId": "subnet-05eef9fb78EXAMPLE",  
"TagSet": [],  
"VpcId": "vpc-0e12f52b21EXAMPLE"  
}  
]  
}
```

Remover prefixos de suas interfaces de rede

É possível remover prefixos de suas interfaces de rede usando um dos métodos a seguir.

Console

Para remover os prefixos de uma interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede da qual remover os prefixos e escolha Ações, Gerenciar prefixos.
4. Execute um destes procedimentos:
 - Para remover todos os prefixos atribuídos, para a Delegação de prefixo IPv4 e Delegação de prefixo IPv6, escolha Não atribuir.
 - Para remover prefixos específicos atribuídos, para Delegação de prefixo IPv4 ou Delegação de prefixo IPv6, escolha Personalizado e, depois, escolha Cancelar atribuição, ao lado dos prefixos a serem removidos.

Note

Delegação de prefixo IPv6 aparece somente se a sub-rede selecionada estiver habilitada para IPv6.

5. Escolha Save (Salvar).

AWS CLI

Você pode usar o `unassign-ipv6-addresses` para remover prefixos IPv6 e o comando `unassign-private-ip-addresses` para remover prefixos IPv4 de suas interfaces de rede existentes.

Para remover prefixos IPv4 de uma interface de rede

Usar a `unassign-private-ip-addresses` Comando e `--ipv4-prefixes` Para o endereço que você deseja remover.

```
C:\> aws ec2 unassign-private-ip-addresses \  
--network-interface-id eni-081fbb4095EXAMPLE \  
--ipv4-prefixes 10.0.0.176/28
```

Para remover prefixos IPv6 de uma interface de rede

Usar o comando `aws ec2 unassign-ipv6-addresses` e o parâmetro `--ipv6-prefix` para o endereço que você deseja remover.

```
C:\> aws ec2 unassign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

Endereços IP elásticos

Um Endereço IP elástico é um endereço IPv4 estático projetado para computação em nuvem dinâmica. Um endereço IP elástico é alocado para a conta da AWS e será seu até que você o libere. Com um endereço IP elástico, é possível mascarar a falha de uma instância ou software remapeando rapidamente o endereço para outra instância na conta. Como alternativa, você pode especificar o endereço IP elástico em um registro DNS para o seu domínio, para que ele acione a sua instância. Para obter mais informações, consulte a documentação do seu registro de domínio.

Um endereço IP elástico é um endereço IPv4 público, que é acessível pela Internet. Se a instância não tiver um endereço IPv4 público, você poderá associar um endereço IP elástico a ela para permitir a comunicação com a Internet. Por exemplo, isso permite que você se conecte à instância do computador local.

No momento, não oferecemos suporte a endereços IP elásticos para IPv6.

Tópicos

- [Definição de preço de endereços IP elásticos \(p. 993\)](#)
- [Noções básicas sobre endereços IP elásticos \(p. 993\)](#)
- [Trabalhar com endereços IP elásticos \(p. 994\)](#)
- [Usar DNS reverso para aplicações de e-mail \(p. 1000\)](#)
- [Limite de endereços IP elásticos \(p. 1001\)](#)

Definição de preço de endereços IP elásticos

Para garantir o uso eficiente de endereços IP elásticos, aplicamos uma pequena cobrança por hora quando um endereço IP elástico não está associado a uma instância em execução ou quando ele está associado a uma instância encerrada ou a uma interface de rede não anexada. Enquanto a instância estiver em execução, você não é cobrado por um endereço IP elástico associado a essa instância, mas será cobrado por qualquer endereço IP elástico adicional associado a ela.

Para obter mais informações, consulte a seção Endereços IP elásticos na página [Pricing \(Definição de preço\) do Amazon EC2, On-Demand Pricing \(Definição de preço sob demanda\)](#).

Noções básicas sobre endereços IP elásticos

As seguintes são as características básicas de um endereço IP elástico:

- Um endereço IP elástico é estático; ele não muda ao longo do tempo.
- Para usar um endereço IP elástico, você primeiro aloca um para sua conta e o associa à instância ou a uma interface de rede.
- Quando você associa um endereço IP elástico a uma instância, ele também é associado à interface de rede principal da instância. Quando você associa um endereço IP elástico a uma interface de rede anexada a uma instância, ele também é associado à instância.

- Quando você associa um endereço IP elástico a uma instância ou à interface de rede principal, o endereço IPv4 público da instância (se existir) é liberado para o grupo de endereços IPv4 públicos da Amazon. Não é possível reutilizar um endereço IPv4 público, nem converter um endereço IPv4 público em um endereço IP elástico. Para obter mais informações, consulte [Endereços IPv4 públicos e nomes de host DNS externos \(p. 957\)](#).
- É possível desassociar um endereço IP elástico de um recurso e reassociá-lo a outro recurso. Para evitar um comportamento inesperado, certifique-se de que todas as conexões ativas com o recurso nomeado na associação existente sejam fechadas antes de fazer a alteração. Depois de associar seu endereço IP elástico a um recurso diferente, será possível reabrir suas conexões com o recurso recém-associado.
- Um endereço IP elástico desassociado permanece alocado à sua conta até você liberá-lo explicitamente. Nós impomos uma pequena cobrança por hora para endereços IP elásticos que não estão associados a uma instância em execução.
- Quando você associa um endereço IP elástico a uma instância que tinha um endereço IPv4 público anteriormente, o nome do host DNS público da instância é alterado para corresponder ao endereço IP elástico.
- Resolvemos o nome DNS do host público para o endereço IPv4 público ou ao endereço IP elástico da instância fora da rede da instância e para o endereço IPv4 privado da instância dentro da rede da instância.
- Um endereço IP elástico é proveniente do grupo de endereços IPv4 públicos da Amazon ou de um grupo de endereços IP personalizados transferido para sua conta da AWS.
- Quando você aloca um endereço IP elástico em um grupo de endereços IP que você levou para sua conta da AWS, ele não é contado nos limites de endereços IP elásticos. Para obter mais informações, consulte [Limite de endereços IP elásticos \(p. 1001\)](#).
- Ao alocar os endereços IP elásticos, é possível associar os endereços IP elásticos a um grupo de borda de rede. Esse é o local a partir do qual anunciamos o bloco CIDR. Definir o grupo de borda de rede limita o bloco CIDR a esse grupo. Se você não especificar o grupo de borda de rede, definiremos o grupo de borda que contém todas as zonas de disponibilidade na região (por exemplo, `us-west-2`).
- Um endereço IP elástico deve ser usado somente um grupo de borda de rede específico.
- Um endereço IP elástico é destinado ao uso somente em uma região específica e não pode ser movido para uma região diferente.

Trabalhar com endereços IP elásticos

As seções a seguir descrevem como você pode trabalhar com endereços IP elásticos.

Tarefas

- [Alocar um endereço IP elástico \(p. 994\)](#)
- [Descrever seus endereços IP elásticos \(p. 996\)](#)
- [Aplicar uma tag em um endereço IP elástico \(p. 996\)](#)
- [Associar um endereço IP elástico a uma instância ou interface de rede \(p. 997\)](#)
- [Dissociar um endereço IP elástico \(p. 998\)](#)
- [Liberar um endereço IP elástico \(p. 999\)](#)
- [Recuperar um endereço IP elástico \(p. 1000\)](#)

Alocar um endereço IP elástico

Você pode alocar um endereço IP elástico no grupo de endereços IPv4 públicos da Amazon ou em um grupo de endereços IP personalizados que você levou para a conta da AWS. Para obter mais informações sobre como levar seu próprio intervalo de endereços IP para sua conta da AWS, consulte [Traga seus próprios endereços IP \(BYOIP\) no Amazon EC2 \(p. 972\)](#).

Você pode alocar um endereço IP elástico usando um dos seguintes métodos.

New console

Para alocar um endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Network & Security (Rede e segurança) e Elastic IPs (IPs elásticos).
3. Escolha Allocate Elastic IP address (Alocar endereço IP elástico).
4. Em Public IPv4 address pool (Grupo de endereços IPv4 público), escolha uma das seguintes opções:
 - Amazon's pool of IPv4 addresses (Grupo de endereços IPv4 da Amazon) — Se você deseja que um endereço IPv4 seja alocado a partir do grupo de endereços IPv4 da Amazon.
 - My pool of public IPv4 addresses (Meu grupo de endereços IPv4 públicos): se você deseja alocar um endereço IPv4 a partir de um grupo de endereços IP que trouxe para sua conta da AWS. Essa opção será desabilitada se você não tiver nenhum pool de endereços IP.
 - Customer owned pool of IPv4 addresses (Grupo de endereços IPv4 de propriedade do cliente): se você quiser alocar um endereço IPv4 de um grupo criado a partir de sua rede on-premises para uso com um AWS Outpost. Essa opção será desativada se você não tiver um Outpost da AWS.
5. (Opcional) Adicione ou remova uma tag.

[Adicionar uma tag] Escolha Adicionar nova tag e faça o seguinte:

- Em Key (Chave), insira o nome da chave.
- Em Value (Valor), insira o valor da chave.

[Remover uma tag] Escolha Remover à direita da chave e do valor da tag.

6. Escolha Allocate.

Old console

Para alocar um endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Escolha Allocate new address.
4. Em IPv4 address pool (Grupo de endereços IPv4), escolha Amazon pool (Grupo da Amazon).
5. Escolha Allocate (Alocar) e feche a tela de confirmação.

AWS CLI

Para alocar um endereço IP elástico

Use o comando da AWS CLI [allocate-address](#).

PowerShell

Para alocar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell [New-EC2Address](#).

Descrever seus endereços IP elásticos

Você pode descrever um endereço IP elástico usando um dos seguintes métodos.

New console

Como descrever seus endereços IP elásticos

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser exibido e escolha Actions (Ações), View details (Exibir detalhes).

Old console

Como descrever seus endereços IP elásticos

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione um filtro na lista de atributos de recursos para começar a pesquisar. Você pode usar vários filtros em uma única pesquisa.

AWS CLI

Como descrever seus endereços IP elásticos

Use o comando da AWS CLI [describe-addresses](#).

PowerShell

Como descrever seus endereços IP elásticos

Use o comando do AWS Tools for Windows PowerShell [Get-EC2Address](#).

Aplicar uma tag em um endereço IP elástico

Você pode atribuir tags personalizadas aos endereços IP elásticos para categorizá-los de diferentes formas, como por objetivo, por proprietário ou por ambiente. Isso ajuda a localizar rapidamente um endereço IP elástico específico baseado em tags personalizadas que você atribuiu a ele.

O rastreamento de alocação de custos usando tags de endereço IP elástico não é compatível.

Você pode marcar um endereço IP elástico usando um dos seguintes métodos.

New console

Para aplicar uma tag em um endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser marcado e escolha Actions (Ações), View details (Exibir detalhes).
4. Na seção Tags, escolha Manage tags (Gerenciar tags).
5. Especifique um par de chave e valor de tag.
6. (Opcional) Escolha Add tag (Adicionar tag) para adicionar outras tags.
7. Escolha Save (Salvar).

Old console

Para aplicar uma tag em um endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico para marcar e selecione Tags.
4. Escolha Add/Edit Tags.
5. Na caixa de diálogo Add/Edit Tags, selecione Create Tag e, em seguida, especifique a chave e o valor da tag.
6. (Opcional) Selecione Create Tag para adicionar tags ao endereço IP elástico.
7. Escolha Save (Salvar).

AWS CLI

Para aplicar uma tag em um endereço IP elástico

Use o comando da AWS CLI [create-tags](#).

```
aws ec2 create-tags --resources eipalloc-12345678 --tags Key=Owner,Value=TeamA
```

PowerShell

Para aplicar uma tag em um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell [New-EC2Tag](#).

O comando New-EC2Tag precisa de um parâmetro de Tag, especificando os pares de chave e valor a serem usados na tag de endereço IP elástico. Os comandos a seguir criam o parâmetro de Tag.

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource eipalloc-12345678 -Tag $tag
```

Associar um endereço IP elástico a uma instância ou interface de rede

Se você está associando um endereço IP elástico à sua instância para habilitar a comunicação com a Internet, deve garantir também que sua instância está em uma sub-rede pública. Para obter mais informações, consulte [Gateways da Internet](#) no Guia do usuário da Amazon VPC.

Você pode associar um endereço IP elástico a uma instância ou interface de rede usando um dos seguintes métodos.

New console

Para associar um endereço Elastic IP a uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser associado e escolha Actions (Ações), Associate Elastic IP address (Associar endereço IP elástico).

4. Em Resource type (Tipo de recurso), escolha Instance (Instância).
5. Por exemplo, escolha a instância à qual associar o endereço IP elástico. Você também pode inserir texto para pesquisar uma instância específica.
6. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.
7. Escolha Associate.

Como associar um endereço IP elástico a uma interface de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser associado e escolha Actions (Ações), Associate Elastic IP address (Associar endereço IP elástico).
4. Em Resource type (Tipo de recurso), selecione Network interface (Interface de rede).
5. Em Network interface (Interface de rede), escolha a interface de rede à qual associar o endereço IP elástico. Você também pode inserir texto para pesquisar uma interface de rede específica.
6. (Opcional) Em Private IP address (Endereço IP privado), especifique um endereço IP privado ao qual associar o endereço IP elástico.
7. Escolha Associate.

Old console

Para associar um endereço Elastic IP a uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione um endereço IP elástico e escolha Actions, Associate address.
4. Selecione a instância em Instance e selecione Associate.

AWS CLI

Como associar um endereço IP elástico

Use o comando da AWS CLI [associate-address](#).

PowerShell

Como associar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell [Register-EC2Address](#).

Dissociar um endereço IP elástico

Você pode desassociar um endereço IP elástico de uma instância ou interface de rede a qualquer momento. Depois de desassociar o endereço IP elástico, você pode reassociá-lo a outro recurso.

Você pode desassociar um endereço IP elástico usando um dos seguintes métodos.

New console

Como desassociar e reassociar um endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser desassociado e escolha Actions (Ações), Disassociate Elastic IP address (Desassociar endereço IP elástico).
4. Escolha Disassociate (Desassociar).

Old console

Como desassociar e reassociar um endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico e escolha Actions e, em seguida, selecione Disassociate address.
4. Escolha Disassociate address.

AWS CLI

Para dissociar um endereço IP elástico

Use o comando da AWS CLI [disassociate-address](#).

PowerShell

Para dissociar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell [Unregister-EC2Address](#).

Liberar um endereço IP elástico

Se você não precisar mais de um endereço IP elástico, recomendamos que o libere usando um dos seguintes métodos. O endereço para lançamento não deve estar associado atualmente a um recurso da AWS, como uma instância do EC2, um gateway NAT ou um平衡ador de carga da rede.

New console

Para liberar um endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico a ser liberado e escolha Actions (Ações), Release Elastic IP addresses (Liberar endereços IP elásticos).
4. Escolha Release (Liberar).

Old console

Para liberar um endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico, escolha Actions e selecione Release addresses. Escolha Release quando solicitado.

AWS CLI

Para liberar um endereço IP elástico

Use o comando da AWS CLI [release-address](#).

PowerShell

Para liberar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell [Remove-EC2Address](#).

Recuperar um endereço IP elástico

Se você divulgou seu Endereço IP elástico, você poderá recuperá-lo. As seguintes regras se aplicam:

- Não é possível recuperar um endereço IP elástico se ele tiver sido alocado a outra conta da AWS, ou se isso resultar em endereços IP elásticos acima do limite.
- Você não pode recuperar tags associadas a um endereço IP elástico.
- Você pode recuperar um endereço IP elástico apenas usando a API do Amazon EC2 ou uma ferramenta de linha de comando.

AWS CLI

Como recuperar um endereço IP elástico

Use o comando da AWS CLI [allocate-address](#) e especifique o endereço IP usando o parâmetro `--address` da seguinte maneira.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

PowerShell

Como recuperar um endereço IP elástico

Use o comando do AWS Tools for Windows PowerShell [New-EC2Address](#) e especifique o endereço IP usando o parâmetro `-Address` da seguinte maneira.

```
PS C:\> New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

Usar DNS reverso para aplicações de e-mail

Se você pretende enviar e-mails a terceiros a partir de uma instância, recomendamos que provisione um ou mais endereços IP elásticos e atribua registros DNS reversos estáticos aos endereços IP elásticos que você usa para enviar e-mails. Isso pode ajudar a evitar que o seu e-mail seja sinalizado como spam por algumas organizações antispam. O AWS trabalha com ISPs e organizações antispam da Internet para reduzir a chance de que e-mails enviados desses endereços sejam sinalizados como spam.

Considerações

- Antes de criar um registro DNS reverso, você deve definir um registro DNS de encaminhamento correspondente (registro do tipo A) que acione o seu endereço IP elástico.
- Se um registro DNS reverso estiver associado a um endereço IP elástico, o endereço IP elástico será bloqueado para sua conta e não poderá ser liberado de sua conta até que o registro seja removido.

Console

Para criar um registro DNS reverso para o seu endereço IP elástico

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs (IPs elásticos).
3. Selecione o endereço IP elástico e escolha Actions (Ações) e Update reverse DNS (Atualizar DNS reverso).
4. Em Reverse DNS domain name (Nome de domínio DNS reverso), insira o nome de domínio a ser associado ao endereço IP elástico.
5. Digite **update** para confirmar.
6. Escolha Update.

AWS CLI

Para criar um registro DNS reverso para o seu endereço IP elástico

- Use o comando [modify-address-attribute](#) AWS CLI para associar o seu nome de domínio ao seu endereço de IP elástico.

AWS GovCloud (US) Region e Regiões da China

Para essas Regiões, você não pode criar um registro DNS reverso usando os métodos acima. AWS deve atribuir os registros DNS reversos estáticos para você. Abra [Solicitar a remoção do DNS reverso e limitações de envio de e-mail](#) e forneça os endereços de IP elásticos e registros DNS reversos.

Limite de endereços IP elásticos

Por padrão, todas as contas da AWS são limitadas a 5 (cinco) endereços IP elásticos por região, pois os endereços públicos da Internet (IPv4) são um recurso público escasso. Recomendamos enfaticamente usar um endereço IP elástico principalmente para a capacidade de remapear o endereço para outra instância no caso de falha da instância, e usar os [nomes de host DNS](#) para qualquer outra comunicação entre nós.

Como verificar quantos endereços IP elásticos estão em uso

Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/> e escolha IPs elásticos no painel de navegação.

Como verificar o limite atual de endereços IP elásticos da conta

É possível verificar seu limite no console do Amazon EC2 ou no console do Service Quotas. Execute um destes procedimentos:

- Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

Escolha Limits (Limites) no painel de navegação e insira **IP** no campo de pesquisa. O limite é EC2-VPC Elastic IPs (IPs elásticos de EC2-VPC). Se você tiver acesso ao EC2-Classic, haverá um limite adicional, EC2-Classic Elastic IPs (IPs elásticos do EC2-Classic).

- Abra o console do Service Quotas em <https://console.aws.amazon.com/servicequotas/>.

No painel, escolha Amazon Elastic Compute Cloud (Amazon EC2). Se o Amazon Elastic Compute Cloud (Amazon EC2) não estiver listado no painel, escolha AWS services (Produtos da AWS), insira **EC2** no campo de pesquisa e escolha Amazon Elastic Compute Cloud (Amazon EC2).

Na página cotas de serviço do Amazon EC2, insira **IP** no campo de pesquisa. O limite é EC2-VPC Elastic IPs (IPs elásticos de EC2-VPC). Se você tiver acesso ao EC2-Classic, haverá um limite adicional, EC2-Classic Elastic IPs (IPs elásticos do EC2-Classic). Para obter mais informações, escolha o limite.

Se achar que a arquitetura justifica endereços IP elásticos adicionais, você poderá solicitar um aumento de cota diretamente no console do Service Quotas.

Interfaces de rede elástica

Uma interface de rede elástica é um componente lógico de redes em uma VPC que representa uma cartão de rede virtual. Ele pode incluir os seguintes atributos:

- Um endereço IPv4 privado primário do intervalo de endereços IPv4 de sua VPC
- Um ou mais endereços IPv4 privados secundários do intervalo de endereços IPv4 de sua VPC
- Um endereço IP elástico (IPv4) por endereço IPv4 privado
- Um endereço IPv4 público
- Um ou mais endereços IPv6
- Um ou mais security groups
- Um endereço MAC
- Um indicador de verificação de origem/destino
- Uma descrição

Você pode criar e configurar interfaces de rede e anexá-las a instâncias na mesma zona de disponibilidade. Sua conta também pode ter interfaces de rede gerenciadas pelo solicitante que são criadas e administradas pelos serviços da AWS, para que você possa usar outros recursos e serviços. Você não pode gerenciar essas interfaces de rede si mesmo. Para obter mais informações, consulte [Interfaces de rede gerenciadas pelo solicitante \(p. 1025\)](#).

Esse recurso da AWS é chamado de interface de rede no AWS Management Console e na API do Amazon EC2. Portanto, usamos "interface de rede" nesta documentação em vez de "interface de rede elástica". O termo "interface de rede" nesta documentação significa sempre "interface de rede elástica".

Tópicos

- [Conceitos básicos da interface de rede \(p. 1002\)](#)
- [Endereços IP por interface de rede por tipo de instância \(p. 1004\)](#)
- [Trabalhar com interfaces de rede \(p. 1015\)](#)
- [Cenários para interfaces de rede \(p. 1023\)](#)
- [Melhores práticas para configurar interfaces de rede \(p. 1025\)](#)
- [Interfaces de rede gerenciadas pelo solicitante \(p. 1025\)](#)

Conceitos básicos da interface de rede

Você pode criar uma interface de rede, associá-la a uma instância, desassociá-la de uma instância e associá-la a outra instância. Os atributos de uma interface de rede a seguem, pois está associada ou desassociada de uma instância e reassociada a outra instância. Quando você move uma interface de rede de uma instância para outra, o tráfego de rede é redirecionado para a nova instância.

Interface de rede primária

Cada instância tem uma interface de rede padrão, chamada interface de rede primária. Você não pode desanexar uma interface de rede primária de uma instância. É possível criar e associar interfaces de rede adicionais. O número máximo de interfaces de rede que você pode usar varia por tipo de instância. Para obter mais informações, consulte [Endereços IP por interface de rede por tipo de instância \(p. 1004\)](#).

Endereços IPv4 públicos para interfaces de rede

Na VPC, todas as sub-redes têm um atributo modificável que determina se às interfaces de rede criadas naquela sub-rede (e, portanto, em instâncias executadas nessa sub-rede) é atribuído um endereço de público IPv4. Para obter mais informações, consulte [Comportamento do endereçamento IP para sua sub-rede](#) no Guia do usuário da Amazon VPC. O endereço IPv4 público é atribuído pelo pool de endereços IPv4 públicos da Amazon. Quando você executa uma instância, o endereço IP é atribuído à interface de rede primária criada.

Ao criar uma interface de rede, ela herda o atributo de endereçamento de IPv4 público da sub-rede. Se você modificar posteriormente o atributo de endereçamento IPv4 público da sub-rede, a interface de rede manterá a configuração vigente de quando ela foi criada. Se você executar uma instância e especificar uma interface de rede existente como a interface de rede primária, o atributo de endereço IPv4 público será determinado por essa interface de rede.

Para obter mais informações, consulte [Endereços IPv4 públicos e nomes de host DNS externos \(p. 957\)](#).

Endereços IP elásticos para interface de rede

Se você tiver um endereço IP elástico, poderá associá-lo a um dos endereços IPv4 privados da interface de rede. Você pode associar um endereço IP elástico a cada endereço IPv4 privado.

Se você desassociar um endereço IP elástico de uma interface de rede, poderá liberá-lo de volta para o grupo de endereços. Essa é a única maneira de associar um endereço IP elástico a uma instância em uma sub-rede ou VPC diferente, já que as interfaces de rede são específicas de sub-redes.

Endereços IPv6 públicos para interfaces de rede

É possível associar blocos CIDR de IPv6 à sua VPC e sub-rede e atribuir um ou mais endereços IPv6 do intervalo de sub-rede a uma interface de rede. Cada endereço IPv6 pode ser atribuído a uma interface de rede.

Todas as sub-redes têm um atributo modificável que determina se às interfaces de rede criadas naquela sub-rede (e, portanto, em instâncias executadas nessa sub-rede) é atribuído automaticamente um endereço de público IPv6 do intervalo da sub-rede. Para obter mais informações, consulte [Comportamento do endereçamento IP para sua sub-rede](#) no Guia do usuário da Amazon VPC. Quando você executa uma instância, o endereço IPv6 é atribuído à interface de rede primária criada.

Para obter mais informações, consulte [Endereços IPv6 \(p. 958\)](#).

Delegação de prefixo

Um prefixo de Delegação de Prefixo é um intervalo de CIDR IPv4 ou IPv6 privado reservado que você aloca para atribuição automática ou manual a interfaces de rede associadas a uma instância. Usando prefixes delegados, você pode iniciar serviços mais rapidamente atribuindo um intervalo de endereços IP como um único prefixo.

Comportamento de encerramento

Você pode definir o comportamento de encerramento para uma interface de rede que está anexada a uma instância. Você pode especificar se a interface de rede deve ser excluída automaticamente quando você encerrar a instância à qual está anexada.

Verificação de origem/destino

Você pode ativar ou desativar as verificações de origem/destino, que garantem que a instância seja a origem ou o destino de qualquer tráfego recebido. A verificação da origem/destino está ativada por padrão.

Você deve desabilitar as verificações de origem/destino se a instância executa serviços como tradução de endereço de rede, roteamento ou firewalls.

Monitoramento do tráfego de IP

Você pode ativar um log de fluxo de VPC na sua interface de rede para capturar informações sobre o tráfego IP que vai e volta da interface de rede. Depois que você tiver criado um log de fluxo, pode visualizar e recuperar esses dados no Amazon CloudWatch Logs. Para obter mais informações, consulte [Logs de fluxo da VPC](#) no Guia do usuário da Amazon VPC.

Endereços IP por interface de rede por tipo de instância

A tabela a seguir lista o número máximo de interfaces de rede por tipo de instância e o número máximo de endereços IPv4 privados e endereços IPv6 por interface de rede. O limite de endereços IPv6 é separado do limite para endereços IPv4 privados por interface de rede. Nem todos os tipos de instância são compatíveis com endereçamento IPv6.

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
c1.medium	2	6	IPv6 não compatível
c1.xlarge	4	15	IPv6 não compatível
c3.large	3	10	10
c3.xlarge	4	15	15
c3.2xlarge	4	15	15
c3.4xlarge	8	30	30
c3.8xlarge	8	30	30
c4.large	3	10	10
c4.xlarge	4	15	15
c4.2xlarge	4	15	15
c4.4xlarge	8	30	30
c4.8xlarge	8	30	30
c5.large	3	10	10
c5.xlarge	4	15	15
c5.2xlarge	4	15	15
c5.4xlarge	8	30	30
c5.9xlarge	8	30	30
c5.12xlarge	8	30	30
c5.18xlarge	15	50	50
c5.24xlarge	15	50	50

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
c5.metal	15	50	50
c5a.large	3	10	10
c5a.xlarge	4	15	15
c5a.2xlarge	4	15	15
c5a.4xlarge	8	30	30
c5a.8xlarge	8	30	30
c5a.12xlarge	8	30	30
c5a.16xlarge	15	50	50
c5a.24xlarge	15	50	50
c5ad.large	3	10	10
c5ad.xlarge	4	15	15
c5ad.2xlarge	4	15	15
c5ad.4xlarge	8	30	30
c5ad.8xlarge	8	30	30
c5ad.12xlarge	8	30	30
c5ad.16xlarge	15	50	50
c5ad.24xlarge	15	50	50
c5d.large	3	10	10
c5d.xlarge	4	15	15
c5d.2xlarge	4	15	15
c5d.4xlarge	8	30	30
c5d.9xlarge	8	30	30
c5d.12xlarge	8	30	30
c5d.18xlarge	15	50	50
c5d.24xlarge	15	50	50
c5d.metal	15	50	50
c5n.large	3	10	10
c5n.xlarge	4	15	15
c5n.2xlarge	4	15	15
c5n.4xlarge	8	30	30

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Endereços IP por interface de rede por tipo de instância

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
c5n.9xlarge	8	30	30
c5n.18xlarge	15	50	50
c5n.metal	15	50	50
cc2.8xlarge	8	30	IPv6 não compatível
cr1.8xlarge	8	30	IPv6 não compatível
d2.xlarge	4	15	15
d2.2xlarge	4	15	15
d2.4xlarge	8	30	30
d2.8xlarge	8	30	30
d3.xlarge	4	3	3
d3.2xlarge	4	5	5
d3.4xlarge	4	10	10
d3.8xlarge	3	20	20
d3en.large	4	2	2
d3en.xlarge	4	3	3
d3en.2xlarge	4	5	5
d3en.4xlarge	4	10	10
d3en.6large	4	15	15
d3en.8xlarge	4	20	20
d3en.12xlarge	3	30	30
f1.2xlarge	4	15	15
f1.4xlarge	8	30	30
f1.16xlarge	8	50	50
g2.2xlarge	4	15	IPv6 não compatível
g2.8xlarge	8	30	IPv6 não compatível
g3s.xlarge	4	15	15
g3.4xlarge	8	30	30
g3.8xlarge	8	30	30
g3.16xlarge	15	50	50
g4ad.xlarge	2	4	4

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
g4ad.2xlarge	2	4	4
g4ad.4xlarge	3	10	10
g4ad.8xlarge	4	15	15
g4ad.16xlarge	8	30	30
g4dn.xlarge	3	10	10
g4dn.2xlarge	3	10	10
g4dn.4xlarge	3	10	10
g4dn.8xlarge	4	15	15
g4dn.12xlarge	8	30	30
g4dn.16xlarge	4	15	15
g4dn.metal	15	50	50
h1.2xlarge	4	15	15
h1.4xlarge	8	30	30
h1.8xlarge	8	30	30
h1.16xlarge	15	50	50
hs1.8xlarge	8	30	IPv6 não compatível
i2.xlarge	4	15	15
i2.2xlarge	4	15	15
i2.4xlarge	8	30	30
i2.8xlarge	8	30	30
i3.large	3	10	10
i3.xlarge	4	15	15
i3.2xlarge	4	15	15
i3.4xlarge	8	30	30
i3.8xlarge	8	30	30
i3.16xlarge	15	50	50
i3.metal	15	50	50
i3en.large	3	10	10
i3en.xlarge	4	15	15
i3en.2xlarge	4	15	15

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Endereços IP por interface de rede por tipo de instância

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
i3en.3xlarge	4	15	15
i3en.6xlarge	8	30	30
i3en.12xlarge	8	30	30
i3en.24xlarge	15	50	50
i3en.metal	15	50	50
m1.small	2	4	IPv6 não compatível
m1.medium	2	6	IPv6 não compatível
m1.large	3	10	IPv6 não compatível
m1.xlarge	4	15	IPv6 não compatível
m2.xlarge	4	15	IPv6 não compatível
m2.2xlarge	4	30	IPv6 não compatível
m2.4xlarge	8	30	IPv6 não compatível
m3.medium	2	6	IPv6 não compatível
m3.large	3	10	IPv6 não compatível
m3.xlarge	4	15	IPv6 não compatível
m3.2xlarge	4	30	IPv6 não compatível
m4.large	2	10	10
m4.xlarge	4	15	15
m4.2xlarge	4	15	15
m4.4xlarge	8	30	30
m4.10xlarge	8	30	30
m4.16xlarge	8	30	30
m5.large	3	10	10
m5.xlarge	4	15	15
m5.2xlarge	4	15	15
m5.4xlarge	8	30	30
m5.8xlarge	8	30	30
m5.12xlarge	8	30	30
m5.16xlarge	15	50	50
m5.24xlarge	15	50	50

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Endereços IP por interface de rede por tipo de instância

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
m5.metal	15	50	50
m5a.large	3	10	10
m5a.xlarge	4	15	15
m5a.2xlarge	4	15	15
m5a.4xlarge	8	30	30
m5a.8xlarge	8	30	30
m5a.12xlarge	8	30	30
m5a.16xlarge	15	50	50
m5a.24xlarge	15	50	50
m5ad.large	3	10	10
m5ad.xlarge	4	15	15
m5ad.2xlarge	4	15	15
m5ad.4xlarge	8	30	30
m5ad.8xlarge	8	30	30
m5ad.12xlarge	8	30	30
m5ad.16xlarge	15	50	50
m5ad.24xlarge	15	50	50
m5d.large	3	10	10
m5d.xlarge	4	15	15
m5d.2xlarge	4	15	15
m5d.4xlarge	8	30	30
m5d.8xlarge	8	30	30
m5d.12xlarge	8	30	30
m5d.16xlarge	15	50	50
m5d.24xlarge	15	50	50
m5d.metal	15	50	50
m5dn.large	3	10	10
m5dn.xlarge	4	15	15
m5dn.2xlarge	4	15	15
m5dn.4xlarge	8	30	30

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
m5dn.8xlarge	8	30	30
m5dn.12xlarge	8	30	30
m5dn.16xlarge	15	50	50
m5dn.24xlarge	15	50	50
m5dn.metal	15	50	50
m5n.large	3	10	10
m5n.xlarge	4	15	15
m5n.2xlarge	4	15	15
m5n.4xlarge	8	30	30
m5n.8xlarge	8	30	30
m5n.12xlarge	8	30	30
m5n.16xlarge	15	50	50
m5n.24xlarge	15	50	50
m5n.metal	15	50	50
m5zn.large	3	10	10
m5zn.xlarge	4	15	15
m5zn.2xlarge	4	15	15
m5zn.3xlarge	8	30	30
m5zn.6xlarge	8	30	30
m5zn.12xlarge	15	50	50
m5zn.metal	15	50	50
m6i.large	3	10	10
m6i.xlarge	4	15	15
m6i.2xlarge	4	15	15
m6i.4xlarge	8	30	30
m6i.8xlarge	8	30	30
m6i.12xlarge	8	30	30
m6i.16xlarge	15	50	50
m6i.24xlarge	15	50	50
m6i.32xlarge	15	50	50

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
p2.xlarge	4	15	15
p2.8xlarge	8	30	30
p2.16xlarge	8	30	30
p3.2xlarge	4	15	15
p3.8xlarge	8	30	30
p3.16xlarge	8	30	30
p3dn.24xlarge	15	50	50
r3.large	3	10	10
r3.xlarge	4	15	15
r3.2xlarge	4	15	15
r3.4xlarge	8	30	30
r3.8xlarge	8	30	30
r4.large	3	10	10
r4.xlarge	4	15	15
r4.2xlarge	4	15	15
r4.4xlarge	8	30	30
r4.8xlarge	8	30	30
r4.16xlarge	15	50	50
r5.large	3	10	10
r5.xlarge	4	15	15
r5.2xlarge	4	15	15
r5.4xlarge	8	30	30
r5.8xlarge	8	30	30
r5.12xlarge	8	30	30
r5.16xlarge	15	50	50
r5.24xlarge	15	50	50
r5.metal	15	50	50
r5a.large	3	10	10
r5a.xlarge	4	15	15
r5a.2xlarge	4	15	15

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
r5a.4xlarge	8	30	30
r5a.8xlarge	8	30	30
r5a.12xlarge	8	30	30
r5a.16xlarge	15	50	50
r5a.24xlarge	15	50	50
r5ad.large	3	10	10
r5ad.xlarge	4	15	15
r5ad.2xlarge	4	15	15
r5ad.4xlarge	8	30	30
r5ad.8xlarge	8	30	30
r5ad.12xlarge	8	30	30
r5ad.16xlarge	15	50	50
r5ad.24xlarge	15	50	50
r5b.large	3	10	10
r5b.xlarge	4	15	15
r5b.2xlarge	4	15	15
r5b.4xlarge	8	30	30
r5b.8xlarge	8	30	30
r5b.12xlarge	8	30	30
r5b.16xlarge	15	50	50
r5b.24xlarge	15	50	50
r5b.metal	15	50	50
r5d.large	3	10	10
r5d.xlarge	4	15	15
r5d.2xlarge	4	15	15
r5d.4xlarge	8	30	30
r5d.8xlarge	8	30	30
r5d.12xlarge	8	30	30
r5d.16xlarge	15	50	50
r5d.24xlarge	15	50	50

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
r5d.metal	15	50	50
r5dn.large	3	10	10
r5dn.xlarge	4	15	15
r5dn.2xlarge	4	15	15
r5dn.4xlarge	8	30	30
r5dn.8xlarge	8	30	30
r5dn.12xlarge	8	30	30
r5dn.16xlarge	15	50	50
r5dn.24xlarge	15	50	50
r5dn.metal	15	50	50
r5n.large	3	10	10
r5n.xlarge	4	15	15
r5n.2xlarge	4	15	15
r5n.4xlarge	8	30	30
r5n.8xlarge	8	30	30
r5n.12xlarge	8	30	30
r5n.16xlarge	15	50	50
r5n.24xlarge	15	50	50
r5n.metal	15	50	50
t1.micro	2	2	IPv6 não compatível
t2.nano	2	2	2
t2.micro	2	2	2
t2.small	3	4	4
t2.medium	3	6	6
t2.large	3	12	12
t2.xlarge	3	15	15
t2.2xlarge	3	15	15
t3.nano	2	2	2
t3.micro	2	2	2
t3.small	3	4	4

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
t3.medium	3	6	6
t3.large	3	12	12
t3.xlarge	4	15	15
t3.2xlarge	4	15	15
t3a.nano	2	2	2
t3a.micro	2	2	2
t3a.small	2	4	4
t3a.medium	3	6	6
t3a.large	3	12	12
t3a.xlarge	4	15	15
t3a.2xlarge	4	15	15
u-6tb1.56xlarge	55	50	50
u-6tb1.112xlarge	155	50	50
u-6tb1.metal	15	50	50
u-9tb1.112xlarge	155	50	50
u-9tb1.metal	15	50	50
u-12tb1.112xlarge	155	50	50
u-12tb1.metal	15	50	50
u-18tb1.metal	15	50	50
u-24tb1.metal	15	50	50
x1.16xlarge	8	30	30
x1.32xlarge	8	30	30
x1e.xlarge	3	10	10
x1e.2xlarge	4	15	15
x1e.4xlarge	4	15	15
x1e.8xlarge	4	15	15
x1e.16xlarge	8	30	30
x1e.32xlarge	8	30	30
z1d.large	3	10	10
z1d.xlarge	4	15	15

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
<code>z1d.2xlarge</code>	4	15	15
<code>z1d.3xlarge</code>	8	30	30
<code>z1d.6xlarge</code>	8	30	30
<code>z1d.12xlarge</code>	15	50	50
<code>z1d.metal</code>	15	50	50

Você pode usar o comando [describe-instance-types](#) (Descrever tipos de instância) da AWS CLI para exibir informações sobre um tipo de instância, como as interfaces de rede compatíveis e os endereços IP por interface. O exemplo a seguir exibe essas informações para todas as instâncias C5.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*" --query "InstanceTypes[].[Type: InstanceType, MaxENI: NetworkInfo.MaximumNetworkInterfaces, IPv4addr: NetworkInfo.Ipv4AddressesPerInterface]" --output table
-----
|      DescribeInstanceTypes      |
+-----+-----+-----+
| IPv4addr | MaxENI | Type   |
+-----+-----+-----+
| 30      | 8      | c5.4xlarge |
| 50      | 15     | c5.24xlarge|
| 15      | 4      | c5.xlarge  |
| 30      | 8      | c5.12xlarge|
| 10      | 3      | c5.large   |
| 15      | 4      | c5.2xlarge |
| 50      | 15     | c5.metal   |
| 30      | 8      | c5.9xlarge |
| 50      | 15     | c5.18xlarge|
+-----+-----+-----+
```

Trabalhar com interfaces de rede

Você pode trabalhar com interfaces de rede usando o console ou a linha de comando do Amazon EC2.

Tópicos

- [Criar uma interface de rede \(p. 1015\)](#)
- [Visualizar detalhes sobre uma interface de rede \(p. 1017\)](#)
- [Anexar uma interface de rede a uma instância. \(p. 1017\)](#)
- [Desanexar uma interface de rede de uma instância \(p. 1018\)](#)
- [Gerenciar endereços IP \(p. 1019\)](#)
- [Modificar atributos da interface de rede \(p. 1020\)](#)
- [Adicionar ou editar tags \(p. 1022\)](#)
- [Excluir uma interface de rede \(p. 1022\)](#)

Criar uma interface de rede

Você pode criar uma interface de rede em uma sub-rede. Não é possível mover a interface de rede para outra sub-rede depois que ela é criada. Você deve associar uma interface de rede a uma instância na mesma zona de disponibilidade.

New console

Para criar uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Clique em Create network interface (Criar interface de rede).
4. (Opcional) Em Description (Descrição), insira um nome descritivo.
5. Em Subnet (Sub-rede), selecione uma sub-rede.
6. Em Private IPv4 address (Endereço IPv4 privado), siga um dos seguintes procedimentos:
 - Clique em Auto-assign (Atribuição automática) para permitir que Amazon EC2 selecione um endereço IPv4 na sub-rede.
 - Clique em Custom (Personalizado) e insira um endereço IPv4 selecionado na sub-rede.
7. (Somente sub-redes com endereços IPv6) Para IPv6 address (Endereço IPv6), execute um dos seguintes procedimentos:
 - Clique em None (Nenhum) se você não quiser atribuir um endereço IPv6 à interface de rede.
 - Clique em Auto-assign (Atribuição automática) para permitir que Amazon EC2 selecione um endereço IPv6 na sub-rede.
 - Clique em Custom (Personalizado) e insira um endereço IPv6 selecionado na sub-rede.
8. (Opcional) Para criar um Elastic Fabric Adapter, clique em Elastic Fabric Adapter e em Enable (Habilitar).
9. Para Security groups, selecione um ou mais security groups.
10. (Opcional) Para cada tag, escolha Add new tag (Adicionar nova tag) e insira uma chave de tag e um valor de tag opcional.
11. Clique em Create network interface (Criar interface de rede).

Old console

Para criar uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Escolha Criar interface de rede.
4. Para Descrição, insira um nome descritivo.
5. Para Sub-rede, selecione a sub-rede.
6. Para IP privado (ou IP IPv4 privado), digite o endereço IPv4 privado primário. Se você não especificar um endereço IPv4, nós selecionaremos um endereço IPv4 privado disponível de dentro da sub-rede selecionada.
7. (Somente IPv6) Se você tiver selecionado uma sub-rede com um bloco CIDR IPv6 associado, é possível especificar um endereço IPv6 no campo IP IPv6.
8. Para criar um Elastic Fabric Adapter, selecione Adaptador de malha elástica.
9. Para Security groups, selecione um ou mais security groups.
10. (Opcional) Escolha Add Tag (Adicionar tag) e digite uma chave de tag e um valor de tag.
11. Escolha Yes, Create.

Para criar uma interface de rede usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [create-network-interface](#) (AWS CLI)
- [New-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Visualizar detalhes sobre uma interface de rede

Você pode visualizar todas as interfaces de rede em sua conta.

New console

Para descrever uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Para exibir a página de detalhes de uma interface de rede, selecione o ID da interface de rede. Como alternativa, para exibir informações sem sair da página de interfaces de rede, marque a caixa de seleção para a interface de rede.

Old console

Para descrever uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede.
4. Para visualizar os detalhes, escolha Details.

Para descrever uma interface de rede usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [describe-network-interfaces](#) (AWS CLI)
- [Get-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Para descrever um atributo de interface de rede usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [describe-network-interface-attribute](#) (AWS CLI)
- [Get-EC2NetworkInterfaceAttribute](#) (AWS Tools for Windows PowerShell)

Anexar uma interface de rede a uma instância.

Você pode associar uma interface de rede a alguma instância na mesma zona de disponibilidade da interface de rede usando o `Instances|Interfaces` de rede na Página do console do Amazon EC2. Se preferir, você pode associar uma interface de rede existente ao [iniciar instâncias \(p. 419\)](#).

Se o endereço IPv4 público da sua instância for liberado, ele não receberá um novo se houver mais de uma interface de rede associada à instância. Para obter mais informações sobre o comportamento dos endereços IPv4 públicos, consulte [Endereços IPv4 públicos e nomes de host DNS externos \(p. 957\)](#).

Instances page

Para anexar uma interface de rede a uma instância usando a página Instances (Instâncias)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Marque a caixa de seleção da instância.
4. Escolha Actions (Ações), Networking (Redes), Attach network interface (Associar interface de rede).
5. Selecione uma interface de rede. Se a instância suportar várias placas de rede, você poderá escolher uma placa de rede.
6. Escolha Associar.

Network Interfaces page

Para associar uma interface de rede a uma instância usando a página Network Interfaces (Interfaces de rede)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações) e em Attach (Associar).
5. Escolha uma instância. Se a instância suportar várias placas de rede, você poderá escolher uma placa de rede.
6. Escolha Associar.

Para associar uma interface de rede à instância usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [attach-network-interface](#) (AWS CLI)
- [Add-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Desanexar uma interface de rede de uma instância

É possível separar uma interface de rede secundária associada a uma instância do EC2 a qualquer momento usando a página Instances (Instâncias) ou Network Interfaces (Interfaces de rede) do console do Amazon EC2.

Se você tentar separar uma interface de rede associada a um recurso de outro serviço, como um load balancer do Elastic Load Balancing, uma função do Lambda, um WorkSpace ou um gateway NAT, você receberá um erro informando que você não tem permissão para acessar o recurso. Para localizar qual serviço criou o recurso anexado a uma interface de rede, verifique a descrição da interface de rede. Se você excluir o recurso, sua interface de rede será excluída.

Instances page

Para separar uma interface de rede de uma instância usando a página Instances

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).

3. Marque a caixa de seleção da instância. Verifique a seção Network interfaces (Interfaces de rede) da guia Networking (Rede) para verificar se a interface de rede está conectada a uma instância como uma interface de rede secundária.
4. Escolha Actions (Ações), Networking (Redes), Detach network interface (Separar interface de rede).
5. Selecione a interface de rede e escolha Separar.

Network Interfaces page

Para separar uma interface de rede de uma instância usando a página Interfaces de rede

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede. Verifique a seção Instance details (Detalhes da instância) da guia Details (Detalhes) para verificar se a interface de rede está conectada a uma instância como uma interface de rede secundária.
4. Clique em Actions (Ações) e em Detach (Desanexar).
5. Quando a confirmação for solicitada, selecione Detach (Desanexar).
6. Se a interface de rede não conseguir se separar da instância, escolha Force detachment (Forçar desanexação), Enable (Ativar) e tente novamente. Recomendamos a desanexação forçada somente como último recurso. Forçar a separação pode impedir que você associe outra interface de rede no mesmo índice até reiniciar a instância. Isso também pode impedir que os metadados da instância reflitam que a interface de rede foi separada até que você reinicie a instância.

Para separar uma interface de rede usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [detach-network-interface](#) (AWS CLI)
- [Dismount-EC2NetworkInterface](#) (AWS Tools for Windows PowerShell)

Gerenciar endereços IP

É possível gerenciar os seguintes endereços IP para suas interfaces de rede:

- Endereços IP elásticos (um por endereço IPv4 privado)
- Endereços IPv4
- Endereços IPv6

Para gerenciar endereços IP elásticos de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Para associar um endereço IP elástico, faça o seguinte:
 - a. Clique em Actions (Ações) e em Associate address (Associar endereço).
 - b. Para Elastic IP address (Endereço IP elástico), selecione o endereço IP elástico.
 - c. Para Private IPv4 address (Endereço IPv4 privado), selecione o endereço IPv4 privado a ser associado ao endereço IP elástico.

- d. (Opcional) Escolha Allow the Elastic IP address to be reassociated (Permitir que o endereço IP elástico seja reassociado) se a interface de rede estiver atualmente associada a outra instância ou interface de rede.
 - e. Escolha Associate.
5. Para desassociar um endereço IP elástico, faça o seguinte:
 - a. Escolha Actions e Disassociate address.
 - b. Em Public IP address (Endereço IP público), selecione o endereço IP elástico.
 - c. Escolha Disassociate (Desassociar).

Como gerenciar os endereços IPv4 e IPv6 de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede.
4. Clique em Actions (Ações) e em Manage IP addresses (Gerenciar endereços IP).
5. Expanda a interface de rede.
6. Para IPv4 addresses (Endereços IPv4), modifique os endereços IP conforme necessário. Para atribuir um endereço IPv4, selecione Assign new IP address (Atribuir novo endereço IP) e especifique um endereço IPv4 do intervalo de sub-rede ou deixe que AWS escolha um para você. Para cancelar a atribuição de um endereço IPv4, escolha Unassign (Desatribuir) ao lado do endereço.
7. Para IPv6 addresses (Endereços IPv6), modifique os endereços IP conforme necessário. Para atribuir um endereço IPv6, escolha Assign new IP (Atribuir novo IP) e especifique um endereço IPv6 do intervalo de sub-rede ou deixe que AWS escolha um para você. Para cancelar a atribuição de um endereço IPv6, escolha Unassign (Desatribuir) ao lado do endereço.
8. Escolha Save (Salvar).

Como gerenciar os endereços IP de uma interface de rede usando a AWS CLI

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [assign-ipv6-addresses](#)
- [associate-address](#)
- [disassociate-address](#)
- [unassign-ipv6-addresses](#)

Como gerenciar os endereços IP de uma interface de rede usando o Tools for Windows PowerShell

Você pode usar um dos comandos a seguir.

- [Register-EC2Address](#)
- [Register-EC2Ipv6AddressList](#)
- [Unregister-EC2Address](#)
- [Unregister-EC2Ipv6AddressList](#)

Modificar atributos da interface de rede

É possível alterar os seguintes atributos de interface de rede:

- [Descrição \(p. 1021\)](#)
- [Grupos de segurança \(p. 1021\)](#)
- [Excluir no encerramento \(p. 1021\)](#)
- [Verificação de origem/destino \(p. 1021\)](#)

Como alterar a descrição de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações) e em Change description (Alterar a descrição).
5. Em Description (Descrição), insira uma descrição para a interface da rede.
6. Escolha Save (Salvar).

Como alterar os grupos de segurança de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações) e em Change security groups (Alterar grupos de segurança).
5. Para Associated security groups (Grupos de segurança associados), selecione os grupos de segurança a serem usados e clique em Save (Salvar).

O grupo de segurança e a interface de rede devem ser criados para a mesma VPC. Para alterar o grupo de segurança para interfaces de propriedade de outros serviços, como o Elastic Load Balancing, faça isso por meio desse serviço.

Como alterar o comportamento de encerramento de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações) e em Change termination behavior (Alterar comportamento de encerramento).
5. Selecione ou desmarque Delete on termination (Excluir no encerramento), Enable (Habilitar) conforme necessário, e depois clique em Save (Salvar).

Para alterar a verificação de origem/destino de uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Clique em Actions (Ações), Change source/dest check (Alterar verificação de origem/destino).

5. Selecione ou desmarque Source/destination check (Verificação de origem/destino), Enable (Habilitar) conforme necessário, e depois clique em Save (Salvar).

Como modificar atributos de interface de rede usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [modify-network-interface-attribute](#) (AWS CLI)
- [Edit-EC2NetworkInterfaceAttribute](#) (AWS Tools for Windows PowerShell)

Adicionar ou editar tags

Tags são metadados que você pode adicionar a uma interface de rede. As tags são privadas e só podem ser vistas pela sua conta. Cada tag consiste em uma chave e um valor opcional. Para obter mais informações sobre tags, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

New console

Para adicionar ou editar tags para uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede.
4. Na guia Tags (Tags), selecione Manage tags (Gerenciar tags).
5. Para cada tag a ser criada, clique em Add new tag (Adicionar nova tag) e insira uma chave e um valor opcional. Quando você terminar, selecione Salvar.

Old console

Para adicionar ou editar tags para uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede.
4. No painel de detalhes, escolha Tags, Adicionar/editar tags.
5. Na caixa de diálogo Adicionar/editar tags, escolha Criar tag para cada tag a ser criada e insira uma chave e um valor opcional. Quando você terminar, selecione Salvar.

Para adicionar ou editar tags para uma interface de rede usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)

Excluir uma interface de rede

A exclusão de uma interface de rede libera todos os atributos associados com a interface e todos os endereços IP privados ou endereços IP elásticos a serem usados por outra instância.

Você não pode excluir uma interface de rede que está em uso. Primeiro, você deve [desanexar a interface de rede \(p. 1018\)](#).

New console

Para excluir uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Marque a caixa de seleção para a interface de rede e selecione Actions (Ações), Delete (Excluir).
4. Quando a confirmação for solicitada, escolha Excluir.

Old console

Para excluir uma interface de rede usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione uma interface de rede e escolha Excluir.
4. Na caixa de diálogo Excluir interface de rede, escolha Sim, excluir.

Para excluir uma interface de rede usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- `delete-network-interface` (AWS CLI)
- `Remove-EC2NetworkInterface` (AWS Tools for Windows PowerShell)

Cenários para interfaces de rede

Associar várias interfaces de rede a uma instância é útil quando você deseja:

- Criar uma rede de gerenciamento.
- Usar dispositivos de rede e segurança na VPC.
- Criar instâncias dual-homed com workloads/funções em sub-redes distintas.
- Criar uma solução de baixo orçamento e alta disponibilidade.

Criar uma rede de gerenciamento.

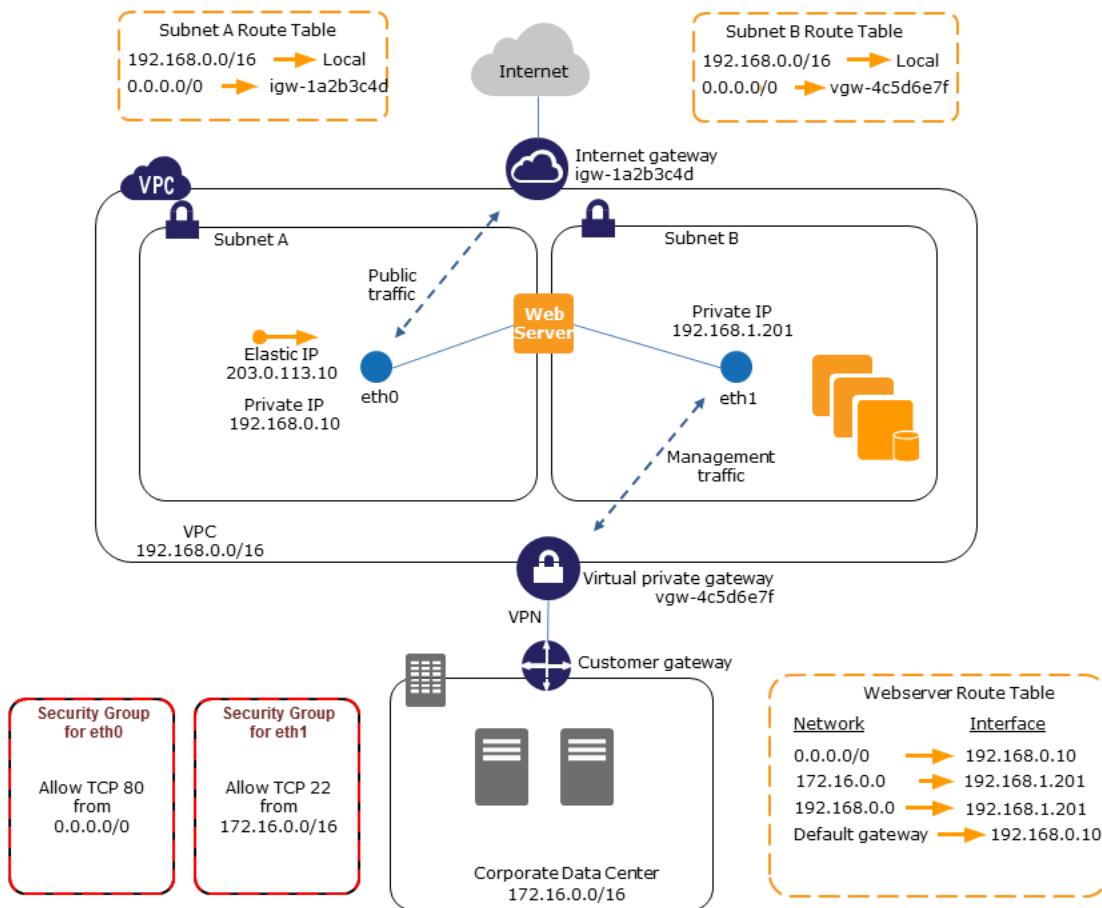
Você pode criar uma rede de gerenciamento usando interfaces de rede. Nesse cenário, conforme ilustrado na imagem a seguir:

- A interface de rede primária (eth0) na instância lida com o tráfego público.
- A interface de rede secundária (eth1) lida com o tráfego de gerenciamento de backend e está conectada a uma sub-rede separada em sua VPC com controles de acesso mais restritivos.

A interface pública, que pode ou não estar atrás de um load balancer, tem um grupo de segurança associado que permite acesso ao servidor a partir da Internet (por exemplo, permitir a porta TCP 80 e 443 em 0.0.0.0/0 ou no load balancer).

A interface privada tem um grupo de segurança associado que permite o acesso RDP apenas em um intervalo permitido de endereços IP, dentro da VPC ou da Internet, uma sub-rede privada dentro da VPC ou um gateway privado virtual.

Para garantir recursos de failover, considere usar um IPv4 privado secundário para o tráfego de entrada em uma interface de rede. No caso de falha de instância, você pode mover a interface e/ou o endereço IPv4 privado secundário para uma instância standby.



Usar dispositivos de rede e segurança na VPC

Algumas ferramentas de rede e segurança, como load balancers, servidores de tradução de endereço de rede (NAT) e servidores proxy preferem ser configurados com várias interfaces de rede. É possível criar e associar interfaces de rede secundárias às instâncias em uma VPC que executa esses tipos de aplicações e configurar interfaces adicionais com seus próprios endereços IP públicos e privados, security groups e verificação de origem/destino.

Criar instâncias dual-homed com workloads/funções em sub-redes distintas

Você pode colocar uma interface de rede em cada um dos servidores Web que se conecta a uma rede mid-tier na qual reside o servidor de aplicações. O servidor de aplicações também pode ser dual-homed para uma rede backend (sub-rede) no servidor onde reside o banco de dados. Em vez de rotear pacotes de rede pelas instâncias dual-homed, cada instância dual-homed recebe e processa solicitações no front-end, inicia uma conexão ao backend e, então, envia solicitações aos servidores na rede backend.

Criar uma solução de baixo orçamento e alta disponibilidade

Se uma das suas instâncias que atende uma função específica falhar, sua interface de rede poderá ser associada a uma instância de substituição ou standby a quente pré-configurada para a mesma função a fim de recuperar rapidamente o serviço. Por exemplo, você pode usar uma interface de rede como interface de rede primária ou secundária para um serviço crítico como uma instância de banco de dados ou instância NAT. Se a instância falhar, você (ou, mais provavelmente, o código em execução em seu nome) pode associar a interface de rede a uma instância de standby a quente. Como a interface mantém os endereços IP privados, endereços IP elásticos e endereço MAC, o tráfego de rede começa a fluir para a instância standby assim que você associar a interface de rede à instância de substituição. Os usuários experimentam uma breve perda de conectividade entre o momento em que a instância falha e a hora em que a interface de rede é associada à instância em standby, mas não é necessária nenhuma alteração na tabela de rotas da VPC no seu servidor DNS.

Melhores práticas para configurar interfaces de rede

- Você pode associar uma interface de rede a uma instância quando ela estiver sendo executada (associação a quente), quando parou (associação em espera ativa) ou quando a instância está sendo executada (associação a frio).
- Você pode desanexar as interfaces de rede secundárias quando a instância estiver sendo executada ou estiver parada. No entanto, não é possível desanexar a interface de rede primária.
- Você pode mover uma interface de rede de uma instância para outra se as instâncias estiverem na mesma zona de disponibilidade e VPC, mas em sub-redes diferentes.
- Ao executar uma instância usando a CLI, a API ou um SDK, é possível especificar a interface de rede primária e interfaces de rede adicionais.
- Executando a instância do Amazon Linux ou do Windows com várias interfaces de rede configura automaticamente interfaces, os endereços IPv4 privados, e tabelas de rotas no sistema operacional da instância.
- Uma associação com espera passiva ou a quente de uma interface de rede adicional pode exigir que você acesse manualmente a segunda interface, configure o endereço IPv4 privado e modifique a tabela de rotas de acordo. As instâncias executadas em Amazon Linux ou Windows Server reconhecem automaticamente a associação com espera passiva ou a quente e se configuram.
- Não é possível associar outra interface de rede a uma instância (por exemplo, uma configuração de teaming de NIC) como método para aumentar ou dobrar a largura de banda quem vem ou vai para a instância dual-homed.
- Se você associar duas ou mais interfaces de rede da mesma sub-rede a uma instância, poderá encontrar problemas de rede, como roteamento assimétrico. Se possível, use um endereço IPv4 privado secundário na interface de rede primária. Se precisar usar várias interfaces de rede, você deverá configurar as interfaces de rede para usar o roteamento estático.

Interfaces de rede gerenciadas pelo solicitante

Uma interface de rede gerenciada pelo solicitante é uma interface de rede que um serviço da AWS cria na sua VPC. Essa interface de rede pode representar uma instância para outro serviço, como uma instância de Amazon RDS, ou pode habilitar o acesso a outro serviço ou recurso, como um serviço de PrivateLink da AWS ou uma tarefa do Amazon ECS.

Uma interface de rede gerenciada pelo solicitante não pode modificada ou desacoplada. Se você excluir o recurso que a interface de rede representa, o serviço da AWS desacopla e exclui interface de rede para você. Para alterar os security groups para uma interface de rede gerenciada pelo solicitante, você pode ter que usar o console ou as ferramentas de linha de comando para esse serviço. Para obter mais informações, consulte a documentação específica do serviço.

Você pode marcar uma interface de rede gerenciada pelo solicitante. Para obter mais informações, consulte [Adicionar ou editar tags \(p. 1022\)](#).

Você pode visualizar as interfaces de rede gerenciadas pelo solicitante que estão em sua conta.

Para visualizar interfaces de rede gerenciadas pelo solicitante usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Selecione a interface de rede e visualize as seguintes informações no painel de detalhes:
 - Attachment owner: Se você criou uma interface de rede, este campo exibe sua ID de conta da AWS. Caso contrário, ele exibe um alias ou uma ID para a entidade ou serviço que criou a interface de rede.
 - Description: Fornece informações sobre o fim de interface de rede; por exemplo, "Interface do VPC endpoint".

Para visualizar interfaces de rede gerenciadas pelo solicitante usando a linha de comando

1. Use o comando [describe-network-interfaces](#) da AWS CLI para descrever as interfaces de rede em sua conta.

```
aws ec2 describe-network-interfaces
```

2. Na saída, se a interface de rede for gerenciada por outro serviço da RequesterManaged, o campo true exibe AWS.

```
{  
    "Status": "in-use",  
    ...  
    "Description": "VPC Endpoint Interface vpce-089f2123488812123",  
    "NetworkInterfaceId": "eni-c8fbc27e",  
    "VpcId": "vpc-1a2b3c4d",  
    "PrivateIpAddresses": [  
        {  
            "PrivateDnsName": "ip-10-0-2-227.ec2.internal",  
            "Primary": true,  
            "PrivateIpAddress": "10.0.2.227"  
        }  
    ],  
    "RequesterManaged": true,  
    ...  
}
```

Alternativamente, use o comando [Get-EC2NetworkInterface](#) do Tools for Windows PowerShell.

Largura de banda de rede de instâncias do Amazon EC2

A largura de banda de rede disponível para uma instância do EC2 depende de vários fatores.

A largura de banda para tráfego multifluxo agregado disponível para uma instância depende do destino do tráfego.

Dentro da Região

O tráfego pode utilizar toda a largura de banda de rede disponível para a instância.

Para outras Regiões, um gateway da Internet ou Direct Connect

O tráfego pode utilizar até 50% da largura de banda de rede disponível para uma [instância da geração atual \(p. 150\)](#) com no mínimo 32 vCPUs. A largura de banda para uma instância de geração atual com menos de 32 vCPUs é limitada a 5 Gbps.

A largura de banda para tráfego de fluxo único (5 tuplas) é limitada a 5 Gbps, independentemente da direção do tráfego. Para casos de uso que exigem baixa latência e alta largura de banda de fluxo único, use um [grupo de posicionamento de cluster \(p. 1044\)](#) para obter largura de banda de até 10 Gbps para instâncias no mesmo grupo de posicionamento. Como alternativa, configure vários caminhos entre dois endpoints para obter maior largura de banda usando MPTCP (Multipath TCP).

Largura de banda disponível da instância

A largura de banda de rede disponível de uma instância depende do número de vCPUs que ela possui. Por exemplo, `ummm5.8xlarge` tem 32 vCPUs e largura de banda de rede de 10 Gbps, e `umam5.16xlarge` tem 64 vCPUs e 20 Gbps de largura de banda de rede. As instâncias podem não atingir essa largura de banda, por exemplo, se excederem as permissões de rede no nível da instância, como pacote por segundo ou número de conexões controladas. A quantidade de largura de banda disponível que o tráfego pode utilizar depende do número de vCPUs e do destino. Por exemplo, uma instância `m5.16xlarge` tem 64 vCPUs, portanto, o tráfego para outra instância na Região pode utilizar a largura de banda total disponível (20 Gbps). No entanto, o tráfego para outra instância em uma Região diferente pode utilizar apenas 50% da largura de banda disponível (10 Gbps).

Normalmente, instâncias com 16 vCPUs ou menos (tamanho `4xlarge` e inferiores) são documentadas como tendo “até” uma largura de banda especificada; por exemplo, “até 10 Gbps”. Essas instâncias têm uma largura de banda de base. Para atender a demanda adicional, eles podem usar um mecanismo de crédito de E/S para explodir além da largura de banda de base. As instâncias podem usar largura de banda intermitente por um tempo limitado, geralmente de 5 a 60 minutos, dependendo do tamanho da instância.

Uma instância recebe o número máximo de créditos de E/S de rede na inicialização. Se a instância esgotar seus créditos de E/S de rede, ela retornará à largura de banda da linha de base. Uma instância em execução ganha créditos de E/S de rede sempre que usa menos largura de banda de rede do que sua largura de banda de base. Uma instância interrompida não ganha créditos de E/S de rede. A intermitência de instância é feita com base no melhor esforço, mesmo quando a instância tem créditos disponíveis, já que a largura de banda intermitente é um recurso compartilhado.

A documentação a seguir descreve a performance da rede para todas as instâncias, além da largura de banda de linha de base disponível para instâncias que podem usar largura de banda intermitente.

- [Instâncias de uso geral \(p. 163\)](#)
- [Instâncias otimizadas para computação \(p. 204\)](#)
- [Instâncias otimizadas para memória \(p. 211\)](#)
- [Instâncias otimizadas para armazenamento \(p. 222\)](#)
- [Instâncias computacionais aceleradas \(p. 231\)](#)

Para exibir a performance da rede usando o AWS CLI

Você pode usar o comando [describe-instance-types](#) da AWS CLI para exibir informações sobre um tipo de instância, como a performance da rede. O exemplo a seguir exibe as informações de performance de redes para todas as instâncias C5.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*" --query "InstanceTypes[].[InstanceType, NetworkInfo.NetworkPerformance]" --output table
|      DescribeInstanceTypes      |
+-----+-----+
| c5.4xlarge | Up to 10 Gigabit |
| c5.xlarge  | Up to 10 Gigabit |
| c5.12xlarge | 12 Gigabit   |
| c5.24xlarge | 25 Gigabit   |
| c5.9xlarge  | 10 Gigabit   |
| c5.2xlarge  | Up to 10 Gigabit |
| c5.large    | Up to 10 Gigabit |
| c5.metal    | 25 Gigabit   |
| c5.18xlarge | 25 Gigabit   |
+-----+-----+
```

Monitorar largura de banda da instância

É possível usar métricas do CloudWatch para monitorar a largura de banda da instância e os pacotes enviados e recebidos. Você pode usar as métricas de performance de rede fornecidas pelo driver Elastic Network Adapter (ENA) para monitorar quando o tráfego excede as permissões de rede definidas pelo Amazon EC2 no nível da instância.

Você pode configurar se o Amazon EC2 envia dados de métrica para a instância ao CloudWatch usando períodos de um ou cinco minutos. É possível que as métricas de performance da rede mostrem que uma permissão foi excedida e os pacotes foram descartados enquanto as métricas da instância do CloudWatch não o fazem. Isso pode acontecer quando a instância tem um pico curto na demanda por recursos de rede (conhecido como micropico de tráfego), mas as métricas do CloudWatch não são detalhadas o suficiente para refletir esses picos de microsegundos.

Saiba mais

- [Métricas de instância \(p. 902\)](#)
- [Métricas de performance da rede \(p. 1041\)](#)

Rede avançada no Windows

A rede avançada usa virtualização de E/S raiz (SR-IOV) para fornecer recursos de rede de alta performance em [tipos de instâncias com suporte \(p. 1029\)](#). A SR-IOV é um método de virtualização de dispositivos que fornece performance de E/S mais elevado e menor utilização de CPU em comparação com interfaces de redes virtualizadas tradicionais. A rede avançada fornece uma largura de banda maior, uma performance melhor de pacotes por segundo (PPS) e latências entre instâncias consistentemente mais baixas. Não há nenhuma cobrança adicional pelo uso da rede avançada.

Para obter mais informações sobre a velocidade de rede compatível com cada tipo de instância, consulte [Tipos de instância do Amazon EC2](#).

Tópicos

- [Suporte a redes avançadas \(p. 1029\)](#)
- [Habilitar redes avançadas na instância \(p. 1029\)](#)
- [Habilitar redes avançadas com o Elastic Network Adapter \(ENA\) em instâncias do Windows \(p. 1029\)](#)
- [Habilitar redes avançadas com a interface Intel 82599 VF nas instâncias do Windows \(p. 1037\)](#)
- [Otimizações do sistema operacional \(p. 1040\)](#)
- [Monitorar a performance de rede de sua instância do EC2 \(p. 1041\)](#)

Suporte a redes avançadas

Todos os tipos de instância da [geração atual \(p. 150\)](#) são compatíveis com redes avançadas, exceto as instâncias T2.

É possível habilitar redes avançadas usando um dos seguintes mecanismos:

Elastic Network Adapter (ENA)

O Elastic Network Adapter (ENA) oferece suporte a velocidades de rede de até 100 Gbps para tipos de instâncias compatíveis.

As instâncias da geração atual usam o ENA para redes avançadas, com exceção das instâncias C4, D2 e M4 menores do que m4.16xlarge.

Interface Intel 82599 Virtual Function (VF)

A interface Intel 82599 Virtual Function oferece suporte a velocidades de rede de até 10 Gbps para tipos de instâncias compatíveis.

Os seguintes tipos de instância usam a interface Intel 82599 VF para redes aprimoradas: C3, C4, D2, I2, M4 (excluindo o m4.16xlarge) e R3.

Para obter um resumo dos mecanismos de redes avançadas por tipo de instância, consulte [Resumo de recursos de redes e armazenamento \(p. 156\)](#).

Habilitar redes avançadas na instância

Se o seu tipo de instância for compatível com o Elastic Network Adapter para rede avançada, siga os procedimentos em [Habilitar redes avançadas com o Elastic Network Adapter \(ENA\) em instâncias do Windows \(p. 1029\)](#).

Se o seu tipo de instância for compatível com a interface Intel 82599 VF para rede avançada, siga os procedimentos em [Habilitar redes avançadas com a interface Intel 82599 VF nas instâncias do Windows \(p. 1037\)](#).

Habilitar redes avançadas com o Elastic Network Adapter (ENA) em instâncias do Windows

O Amazon EC2 oferece recursos de rede avançada pelo Elastic Network Adapter (ENA). Para usar a rede aprimorada, é necessário instalar o módulo ENA necessário e habilitar o suporte ENA.

Tópicos

- [Requirements \(p. 1029\)](#)
- [Performance da rede avançada \(p. 1030\)](#)
- [Testar se a rede avançada está habilitada \(p. 1030\)](#)
- [Habilitar redes avançadas no Windows \(p. 1031\)](#)
- [Versões do driver do Amazon ENA \(p. 1032\)](#)
- [Assinar notificações do \(p. 565\)](#)

Requirements

Para se preparar para a rede avançada com o ENA, configure a instância da seguinte forma:

- Execute a instância usando um tipo de instância da [geração atual \(p. 150\)](#) que seja diferente das instâncias C4, D2 e M4 menores do que m4.16xlarge ou T2.
- Se a instância estiver executando o Windows Server 2008 R2 SP1, verifique se ela tem a [atualização de suporte de assinatura de código SHA-2](#).
- Verifique se a instância tem conectividade com a Internet.
- Use o [AWS CloudShell](#) do AWS Management Console ou instale e configure a [AWS CLI](#) ou o [AWS Tools for Windows PowerShell](#) em qualquer computador de sua escolha, preferivelmente, em seu desktop ou laptop local. Para obter mais informações sobre o ACM, consulte [Acessar o Amazon EC2 \(p. 3\)](#) ou o [Guia do usuário do AWS CloudShell](#). A rede avançada não pode ser gerenciada no console do Amazon EC2.
- Se houver dados importantes na instância que deseja preservar, você deverá fazer backup desses dados agora criando uma AMI na instância. A atualização de kernels e módulos de kernel e a habilitação do atributo enaSupport podem renderizar instâncias incompatíveis ou sistemas operacionais inacessíveis. Se você tiver um backup recente, seus dados ainda serão retidos, caso isso ocorra.

Performance da rede avançada

A documentação a seguir fornece um resumo da performance da rede para os tipos de instância que oferecem suporte às redes avançadas do ENA:

- [Performance de rede para Instâncias computacionais aceleradas \(p. 231\)](#)
- [Performance de rede para instâncias otimizadas para computação \(p. 207\)](#)
- [Performance de rede para instâncias de uso geral \(p. 163\)](#)
- [Performance de rede para instâncias otimizadas para memória \(p. 216\)](#)
- [Performance de rede para instâncias otimizadas para armazenamento \(p. 225\)](#)

Testar se a rede avançada está habilitada

Para testar se a rede avançada já está habilitada, verifique se o driver está instalado na instância e se o atributo enaSupport está definido.

Atributo de instância (enaSupport)

Para verificar se uma instância tem o atributo enaSupport de rede avançada definido, use um dos seguintes comandos. Se o atributo estiver definido, a resposta será verdadeira.

- [describe-instances](#) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query  
"Reservations[].[Instances[].[EnaSupport"]"
```

- [Get-EC2Instance](#) (Tools for Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

Atributo de imagem (enaSupport)

Para verificar se uma AMI tem o atributo enaSupport de rede avançada definido, use um dos seguintes comandos. Se o atributo estiver definido, a resposta será verdadeira.

- [describe-images](#) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[ ].EnaSupport"
```

- [Get-EC2Image](#) (Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami_id).EnaSupport
```

Habilitar redes avançadas no Windows

Se você executou a instância e ela ainda não tiver a rede avançada habilitada, você deverá fazer download e instalar o driver do adaptador de rede necessário na instância e, em seguida, definir o atributo `enaSupport` da instância para ativar a rede avançada. Você somente poderá ativar esse atributo em tipos de instância suportados e somente se o driver ENA estiver instalado. Para obter mais informações, consulte [Suporte a redes avançadas \(p. 1029\)](#).

Para habilitar a rede avançada

1. Conecte-se à instância e faça login como administrador local.
2. [Windows Server 2016 e posterior somente] Execute o seguinte script do PowerShell do EC2Launch para configurar a instância depois de instalar o driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -  
Schedule
```

3. Na instância, instale o driver da seguinte forma:
 - a. [Faça download](#) do driver mais recente para a instância.
 - b. Extraia o arquivo zip.
 - c. Instale o driver executando o script `install.ps1` do PowerShell.

Note

Se você receber um erro de política de execução, defina a política como `Unrestricted` (por padrão, ela é definida como `Restricted` ou `RemoteSigned`). Em uma linha de comando, execute `Set-ExecutionPolicy -ExecutionPolicy Unrestricted` e, depois, execute o script `install.ps1` do PowerShell novamente.

4. No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: `stop-instances` (AWS CLI/AWS CloudShell), [Stop-EC2Instance](#) (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, você deve parar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
5. Ative o suporte ao ENA na instância da seguinte maneira:

- a. No computador local, verifique o atributo de suporte ao ENA da instância do EC2 em sua instância executando um dos seguintes comandos. Se o atributo não estiver habilitado, a saída será “[]” ou em branco. `EnaSupport` será definido como `false` por padrão.
 - [describe-instances](#) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query  
"Reservations[ ].Instances[ ].EnaSupport"
```

- [Get-EC2Instance](#) (Tools para Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance_id).Instances.EnaSupport
```

- b. Para ativar o suporte ao ENA, execute um dos seguintes comandos:

- [modify-instance-attribute](#) (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

Se encontrar problemas ao reiniciar a instância, você também poderá desativar o suporte ao ENA com um dos seguintes comandos:

- [modify-instance-attribute](#) (AWS CLI/AWS CloudShell)

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
```

- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $false
```

- c. Verifique se o atributo foi definido como `true` usando `describe-instances` ou `Get-EC2Instance` conforme mostrado anteriormente. Você agora deve ver a seguinte saída:

```
[  
    true  
]
```

6. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: [start-instances](#) (AWS CLI/AWS CloudShell), [Start-EC2Instance](#) (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, você deverá iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
7. Na instância, valide se o driver do ENA está instalado e ativado da seguinte maneira:
 - Clique com o botão direito do mouse no ícone de rede e escolha Abrir Central de Rede e Compartilhamento.
 - Escolha o adaptador de Ethernet (por exemplo, Ethernet 2).
 - Escolha Detalhes. Para Detalhes da conexão de rede, verifique se a Descrição é Amazon Elastic Network Adapter.
8. (Opcional) Crie uma AMI na instância. A AMI herda o atributo `enaSupport` da instância. Portanto, você pode usar essa AMI para executar outra instância com ENA ativado por padrão. Para obter mais informações, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#).

Versões do driver do Amazon ENA

As AMIs do Windows incluem o driver do Amazon ENA para habilitar a rede avançada. A tabela a seguir resume as alterações de cada versão.

Versão do driver	Detalhes	Data de lançamento
2.2.3	<p>Novo recurso</p> <ul style="list-style-type: none">Adiciona suporte para novos Nitro Cards com rede de instâncias de até 400 Gbps.	25 de março de 2021

Versão do driver	Detalhes	Data de lançamento
	<p>Correção de bugs</p> <ul style="list-style-type: none"> Corrigir um comportamento de disputa entre a mudança de hora do sistema e a consulta de hora do sistema pelo driver do ENA, que causa a detecção falso-positiva de falta de resposta de HW. 	
2.2.2	<p>Novo recurso</p> <ul style="list-style-type: none"> Adiciona suporte para consultar métricas de performance do adaptador de rede com o CloudWatch e os Contadores de performance para consumidores do Windows. <p>Correção de bugs</p> <ul style="list-style-type: none"> Corrigir problemas de performance em instâncias bare metal. 	21 de dezembro de 2020
2.2.1	<p>Novo recurso</p> <ul style="list-style-type: none"> Adiciona um método para permitir que o host consulte o Elastic Network Adapter para obter métricas de performance da rede. 	1º de outubro de 2020
2.2.0	<p>Novos recursos</p> <ul style="list-style-type: none"> Adiciona suporte aos tipos de hardware de próxima geração. Melhora o tempo de inicialização da instância após retomar de uma parada de hibernação e elimina mensagens de erro de falsos positivos de ENA. <p>Otimizações da performance</p> <ul style="list-style-type: none"> Otimiza o processamento do tráfego de entrada. Melhora o gerenciamento de memória compartilhada em um ambiente de recursos escassos. <p>Correção de bugs</p> <ul style="list-style-type: none"> Evita a falha do sistema após a remoção do dispositivo do ENA em um cenário raro em que há falha na redefinição do driver. 	12 de agosto de 2020
2.1.5	<p>Correção de bugs</p> <ul style="list-style-type: none"> Corrigir falhas ocasionais de inicialização do adaptador de rede em instâncias bare metal. 	23 de junho de 2020

Versão do driver	Detalhes	Data de lançamento
2.1.4	<p>Correções de bugs</p> <ul style="list-style-type: none"> Evite problemas de conectividade causados por metadados de pacotes LSO corruptos chegando da pilha da rede. Evite falha no sistema causada por uma condição de corrida rara que resulta no acesso de uma memória de pacote já liberada. 	25 de novembro de 2019
2.1.2	<p>Novo recurso</p> <ul style="list-style-type: none"> Adição de suporte para que o relatório do ID do fornecedor permita que o SO gere UUIDs baseadas em MAC. <p>Correções de bugs</p> <ul style="list-style-type: none"> Melhoria na performance da configuração de rede DHCP durante a inicialização. Calcule corretamente a soma de verificação L4 no tráfego IPv6 de entrada quando a unidade de transmissão máxima (MTU) exceder 4K. Melhorias gerais na estabilidade do driver e correções de erros secundárias. 	4 de novembro de 2019
2.1.1	<p>Correções de bugs</p> <ul style="list-style-type: none"> Previnem a chegada de pacotes LSO TCP altamente fragmentados do sistema operacional. Lidam corretamente com o protocolo Encapsulating Security Payload (ESP) dentro do IPSec em redes IPv6. 	16 de setembro de 2019

Versão do driver	Detalhes	Data de lançamento
2.1.0	<p>O driver ENA v2.1 do Windows apresenta novos recursos do dispositivo ENA, dá um impulso à performance, adiciona novos recursos e inclui várias melhorias de estabilidade.</p> <ul style="list-style-type: none"> • Novos recursos <ul style="list-style-type: none"> • Use a chave do Registro do Windows padronizada para configuração dos frames jumbo. • Permitir a configuração do ID da VLAN via a GUI das propriedades do driver ENA. • Fluxos de recuperação melhorados <ul style="list-style-type: none"> • Melhora no mecanismo de identificação de falhas. • Adicionado suporte para parâmetros de recuperação ajustáveis. • Compatibilidade para até 32 filas de E/S para instâncias do EC2 mais novas, que têm mais de 8 vCPUs. • Redução de ~90% da presença de memória do driver. • Otimizações da performance <ul style="list-style-type: none"> • Redução na latência do caminho de transmissão. • Suporte para receber o descarregamento da soma de verificação. • Otimização da performance para um sistema pesadamente carregado (uso otimizado dos mecanismos de bloqueio). • Outras melhorias para reduzir a utilização da CPU e melhorar a responsividade do sistema em carga. • Correções de bugs <ul style="list-style-type: none"> • Corrigir a falha devido à análise inválida de cabeçalhos Tx não contíguos. • Corrigir a falha do driver v1.5 durante a desanexação da ENI em instâncias bare metal. • Corrigir o erro de cálculo da soma de verificação do pseudocabeçalho do LSO sobre IPv6. • Corrigir o vazamento de recursos de memória em potencial na falha da inicialização. • Desabilitar o descarregamento da soma de verificação de TCP/UDP para fragmentos de IPv4. • Corrigir para configuração da VLAN. A VLAN foi desabilitada incorretamente quando somente a prioridade da VLAN deveria ter sido desabilitada. • Habilitar a análise das mensagens do driver personalizado pelo visualizador de eventos. • Corrigir a falha em inicializar o driver devido a tratamento de timestamp inválido. • Corrigir a condição da corrida entre o processamento de dados e a desabilitação do dispositivo ENA. 	1 de julho de 2019

Versão do driver	Detalhes	Data de lançamento
1.5.0	<ul style="list-style-type: none"> Estabilidade aprimorada e correções de performance. Os buffers de recebimento agora podem ser configurados até um valor de 8192 em Advanced Properties (Propriedades avançadas) de NIC do ENA. Buffers de recebimento padrão de 1 k. 	4 de outubro de 2018
1.2.3	Inclui correções de confiabilidade e unifica o suporte para o Windows Server 2008 R2 por meio do Windows Server 2016.	13 de fevereiro de 2018
1.0.9	Inclui algumas correções de confiabilidade. Aplica-se apenas ao Windows Server 2008 R2. Não recomendada para outras versões do Windows Server.	º de dezembro de 2016
1.0.8	A versão inicial. Incluída em AMIs do Windows Server 2008, do Windows Server 2012 RTM, do Windows Server 2012 R2 e do Windows Server 2016.	Julho de 2016

Assinar notificações do

O Amazon SNS pode notificá-lo quando novas versões dos drivers EC2 para Windows são lançadas. Use o procedimento a seguir para se inscrever nessas notificações.

Para assinar as notificações do EC2

1. Abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.
2. Na barra de navegação, altere a região para Leste dos EUA (Norte da Virgínia), se necessário. É necessário selecionar esta região porque as notificações do SNS que você está assinando estão nesta região.
3. No painel de navegação, escolha Subscriptions.
4. Selecione Create subscription.
5. Na caixa de diálogo Criar assinatura, faça o seguinte:
 - a. Para o ARN do tópico, copie o seguinte ARN (nome de recurso da Amazon):


```
arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
```
 - b. Para Protocolo, selecione Email.
 - c. Em Endpoint, insira um endereço de e-mail que possa ser usado para receber notificações.
 - d. Selecione Create subscription.
6. Você receberá um e-mail de confirmação. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Sempre que novos drivers EC2 para Windows são lançados, nós enviamos notificações aos assinantes. Se não deseja mais receber essas notificações, use o procedimento a seguir para cancelar a assinatura.

Para cancelar a assinatura de notificações do driver Amazon EC2 para Windows

1. Abra o console do Amazon SNS em <https://console.aws.amazon.com/sns/v3/home>.
2. No painel de navegação, escolha Subscriptions.
3. Marque a caixa de seleção da assinatura e, depois, selecione Actions (Ações), Delete subscriptions (Excluir assinaturas). Quando a confirmação for solicitada, escolha Excluir.

Habilitar redes avançadas com a interface Intel 82599 VF nas instâncias do Windows

O Amazon EC2 fornece recursos de redes avançadas por meio da interface Intel 82599 VF, que usa o driver `ixgbevf` da Intel.

Tópicos

- [Requirements \(p. 1037\)](#)
- [Testar se a rede avançada está habilitada \(p. 1037\)](#)
- [Habilitar a rede avançada no Windows \(p. 1038\)](#)

Requirements

Para se preparar para a rede avançada com a interface Intel 82599 VF, configure a instância da seguinte forma:

- Selecione um dos seguintes tipos de instância compatíveis: C3, C4, D2, I2, M4 (exceto `m4.16xlarge`) e R3.
- Executar a instância a partir da AMI de HVM de 64 bits. Você não pode habilitar uma rede avançada no Windows Server 2008 e no Windows Server 2003. A rede avançada já está habilitada para AMIs do Windows Server 2012 R2 e do Windows Server 2016 e posterior. O Windows Server 2012 R2 inclui o driver 1.0.15.3 da Intel e recomendamos atualizar esse driver para a versão mais recente usando o utilitário Pnutil.exe.
- Verifique se a instância tem conectividade com a Internet.
- Use o [AWS CloudShell](#) do AWS Management Console ou instale e configure a [AWS CLI](#) ou o [AWS Tools for Windows PowerShell](#) em qualquer computador de sua escolha, preferivelmente, em seu desktop ou laptop local. Para obter mais informações sobre o ACM, consulte [Acessar o Amazon EC2 \(p. 3\)](#) ou o [Guia do usuário do AWS CloudShell](#). A rede avançada não pode ser gerenciada no console do Amazon EC2.
- Se houver dados importantes na instância que deseja preservar, você deverá fazer backup desses dados agora criando uma AMI na instância. A atualização de kernels e módulos de kernel e a habilitação do atributo `sriovNetSupport` podem renderizar instâncias incompatíveis ou sistemas operacionais inacessíveis. Se você tiver um backup recente, seus dados ainda serão retidos, caso isso ocorra.

Testar se a rede avançada está habilitada

A rede avançada com a interface Intel 82599 VF já estará habilitada se o driver do módulo estiver instalado na instância e se o atributo `sriovNetSupport` está definido.

Driver

Para verificar se o driver está instalado, conecte-se à instância e abra o Gerenciador de dispositivos. Você deve ver a “Intel (R) 82599 Virtual Function” listada em Network adapters.

Atributo de instância (`sriovNetSupport`)

Para verificar se uma instância tem o atributo `sriovNetSupport` de rede avançada definido, use um dos seguintes comandos:

- [describe-instance-attribute \(AWS CLI/AWS CloudShell\)](#)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute sriovNetSupport
```

- [Get-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute sriovNetSupport
```

Se o atributo não estiver definido, o `SriovNetSupport` estará vazio. Se o atributo for definido, o valor será simples, como mostrado na saída de exemplo a seguir.

```
"SriovNetSupport": {  
    "Value": "simple"  
},
```

Atributo de imagem (`sriovNetSupport`)

Para verificar se uma AMI já tem o atributo `sriovNetSupport` de rede avançada definido, use um dos seguintes comandos:

- [describe-images](#) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[].[SriovNetSupport]"
```

- [Get-EC2Image](#) (AWS Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami-id).SriovNetSupport
```

Se o atributo não estiver definido, o `SriovNetSupport` estará vazio. Se o atributo for definido, o valor será simples.

Habilitar a rede avançada no Windows

Se você executou a instância e ela ainda não tiver a rede avançada habilitada, você deverá fazer download e instalar o driver do adaptador de rede necessário na instância e, em seguida, definir o atributo `sriovNetSupport` da instância para ativar a rede avançada. Você só pode habilitar esse atributo em tipos de instâncias compatíveis. Para obter mais informações, consulte [Suporte a redes avançadas \(p. 1029\)](#).

Important

Para ver a versão mais recente do driver Intel nas AMIs do Windows, consulte [Detalhes sobre versões de AMI do Windows da AWS \(p. 31\)](#).

Warning

Não há nenhuma maneira de desabilitar o atributo de rede avançada depois de ele ser habilitado.

Para habilitar a rede avançada

1. Conecte-se à instância e faça login como administrador local.
2. [Windows Server 2016 e posterior] Execute o seguinte script do PowerShell do EC2Launch para configurar a instância depois de instalar o driver.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -  
Schedule
```

Important

A senha do administrador será redefinida quando você habilitar o script de inicialização do EC2Launch da instância. Você pode modificar o arquivo de configuração para desabilitar a redefinição da senha do administrador especificando-a nas configurações das tarefas de inicialização. Para obter as etapas sobre como desabilitar a redefinição de senha, consulte [Configurar as tarefas de inicialização \(p. 524\)](#).

3. Na instância, faça download do driver do adaptador de rede da Intel para seu sistema operacional:
 - Windows Server 2019, inclusive para a versão de servidor 1809 e posterior*
Visite a [página de download](#) e faça download do `Wired_driver_version_x64.zip`.
 - Windows Server 2016, inclusive para a versão de servidor 1803 e anterior*
Visite a [página de download](#) e faça download do `Wired_driver_version_x64.zip`.
 - Windows Server 2012 R2
Visite a [página de download](#) e faça download do `Wired_driver_version_x64.zip`.
 - Windows Server 2012
Visite a [página de download](#) e faça download do `Wired_driver_version_x64.zip`.
 - Windows Server 2008 R2
Visite a [página de download](#) e faça download do `PROWinx64Legacy.exe`.

*As versões de servidor 1803 e anteriores, bem como a 1809 e posterior, não são especificamente abordadas nas páginas de Drivers e Software da Intel.

4. Instale o driver do adaptador de rede da Intel para seu sistema operacional:
 - Windows Server 2008 R2
 1. Na pasta Downloads, localize o arquivo `PROWinx64Legacy.exe` e renomeie-o como `PROWinx64Legacy.zip`.
 2. Extraia o conteúdo do arquivo `PROWinx64Legacy.zip`.
 3. Abra a linha de comando, navegue até a pasta com os arquivos extraídos e execute o comando a seguir a fim de usar o utilitário `pnputil` para adicionar e instalar o arquivo INF no armazenamento de drivers.

```
C:\> pnputil -a  
PROXGB\Winx64\NDIS62\vxn62x64.inf.
```

- Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 e Windows Server 2012
 - 1. Na pasta Downloads, extraia o conteúdo do arquivo `Wired_driver_version_x64.zip`.
 - 2. Na pasta com arquivos extraídos, localize o arquivo `Wired_driver_version_x64.exe` e renomeie-o como `Wired_driver_version_x64.zip`.
 - 3. Extraia o conteúdo do arquivo `Wired_driver_version_x64.zip`.
 - 4. Abra a linha de comando, navegue até a pasta com os arquivos extraídos e execute os comandos a seguir a fim de usar o utilitário `pnputil` para adicionar e instalar o arquivo INF no armazenamento de drivers.
- Windows Server 2019

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
```

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
```

- Windows Server 2012 R2

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
```

- Windows Server 2012

```
C:\> pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
```

5. No computador local, interrompa a instância usando o console do Amazon EC2 ou um dos seguintes comandos: [stop-instances](#) (AWS CLI), [Stop-EC2Instance](#) (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, você deve parar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
 6. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:
 - [modify-instance-attribute](#) (AWS CLI/AWS CloudShell)
- ```
aws ec2 modify-instance-attribute --instance-id instance_id --srivnet-support simple
```
- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)
- ```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```
7. (Opcional) Crie uma AMI na instância, conforme descrito em [Criar uma AMI do Windows personalizada \(p. 39\)](#). A AMI herda o atributo da rede avançada da instância. Portanto, você pode usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.
 8. No computador local, inicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: [start-instances](#) (AWS CLI), [Start-EC2Instance](#) (AWS Tools for Windows PowerShell). Se sua instância for gerenciada por AWS OpsWorks, você deve iniciar a instância no console do AWS OpsWorks de modo que o estado da instância permaneça sincronizado.
- ## Otimizações do sistema operacional
- Para obter a máxima performance da rede em instâncias com redes avançadas, pode ser necessário modificar a configuração do sistema operacional padrão. Recomendamos as seguintes alterações de configuração para aplicações que exigem alta performance de rede. Outras otimizações (como ativar o descarregamento de soma de verificação e a ativação do RSS, por exemplo) já estão em vigor em AMIs oficiais do Windows.
- ### Note
- O descarregamento do TCP chimney deve ser desabilitado na maioria dos casos de uso e se tornou obsoleto a partir do Windows Server 2016.
- Além dessas otimizações do sistema operacional, você também deve considerar a unidade de transmissão máxima (MTU - maximum transmission unit) de seu tráfego de rede e ajustá-la de acordo com sua workload e arquitetura de rede. Para obter mais informações, consulte [Unidade de transmissão máxima \(MTU\) de rede para a instância do EC2 \(p. 1056\)](#).
- AWSA mede regularmente as latências médias de ida e volta entre instâncias iniciadas em um placement group de cluster de 50us e latência final de 200us no percentil 99,9. Se suas aplicações exigirem baixas latências de forma consistente, recomendamos usar a versão mais recente dos drivers ENA em instâncias de performance fixa criadas no sistema Nitro.
- 1040

Configurar afinidade de CPU RSS

O Receive Side Scaling (RSS) é usado para distribuir a carga da CPU do tráfego de rede em vários processadores. Por padrão, as AMIs oficiais do Amazon Windows são configuradas com RSS ativado. ENIs do ENA fornecem até oito filas RSS. Com a definição de afinidade de CPU para filas RSS, bem como para outros processos do sistema, é possível distribuir a carga de CPU pelos sistemas com vários núcleos, permitindo que mais tráfego de rede seja processado. Em tipos de instância com mais de 16 vCPUs, recomendamos usar o cmdlt do PowerShell Set-NetAdapterRSS (disponível no Windows Server 2012 e posterior), que exclui manualmente o processador de inicialização (processador lógico 0 e 1 quando o hyper-threading está habilitado) da configuração RSS de todas as ENIs, a fim de evitar a contenção com vários componentes do sistema.

O Windows reconhece o hyper-thread e garantirá que as filas RSS de uma única NIC sejam sempre colocadas em diferentes núcleos físicos. Portanto, a menos que o hyper-threading esteja desabilitado, para evitar completamente a contenção com outras NICs, propague a configuração RSS de cada NIC entre um intervalo de 16 processadores lógicos. O cmdlt Set-NetAdapterRss permite que você defina o intervalo por NIC de processadores lógicos válidos definindo os valores de BaseProcessorGroup, BaseProcessorNumber, MaxProcessingGroup, MaxProcessorNumber e NumaNode (opcional). Se não houver núcleos físicos suficientes para eliminar completamente a contenção entre NICs, minimize os intervalos de sobreposição ou reduza o número de processadores lógicos nos intervalos de ENI dependendo da workload esperada da ENI (ou seja, uma ENI de rede administrativa de baixo volume pode não precisar de tantas filas RSS atribuídas). Além disso, como observado acima, diversos componentes devem ser executados na CPU 0 e, por isso, recomendamos a exclusão em todas as configurações RSS quando houver vCPUs suficientes disponíveis.

Por exemplo, quando há três ENIs em uma instância de 72 vCPUs com 2 nós NUMA com o hyper-threading habilitado, os comandos a seguir distribuem a carga de rede entre as duas CPUs sem sobreposição e impedem completamente o uso do núcleo 0.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -  
MaxProcessorNumber 16  
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -  
MaxProcessorNumber 14  
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -  
MaxProcessorNumber 30
```

Observe que essas configurações são persistentes para cada adaptador de rede. Se uma instância for redimensionada para uma com um número diferente de vCPUs, você deverá reavaliar a configuração RSS para cada ENI habilitada. A documentação completa da Microsoft para o cmdlt Set-NetAdapterRss pode ser encontrada aqui: <https://docs.microsoft.com/en-us/powershell/module/netadapter/set-netadapterrss>.

Observação especial para workloads SQL: também recomendamos que você revise suas configurações de afinidade de thread de E/S juntamente com sua configuração RSS da ENI para minimizar a contenção de E/S e de rede para as mesmas CPUs. Consulte [Opção de configuração do servidor de máscara de afinidade](#).

Monitorar a performance de rede de sua instância do EC2

O driver Elastic Network Adapter (ENA) publica métricas de performance de rede com base nas instâncias em que elas estão habilitadas. Você pode usar essas métricas para solucionar problemas de performance da instância, escolher o tamanho certo da instância para uma workload, planejar atividades de dimensionamento proativamente e comparar aplicações para determinar se eles maximizam a performance disponível em uma instância.

O Amazon EC2 define os máximos de rede no nível da instância para garantir uma experiência de rede de alta qualidade, incluindo performance consistente da rede entre tamanhos de instância. A AWS fornece máximos para o seguinte para cada instância:

- Capacidade de largura de banda: cada instância do EC2 tem uma largura de banda máxima para tráfego agregado de entrada e saída, com base no tipo e no tamanho da instância. Algumas instâncias usam um mecanismo de crédito de E/S para alocar a largura de banda da rede com base na utilização média da largura de banda. O Amazon EC2 também tem largura de banda máxima para tráfego para AWS Direct Connect e a Internet.
- Performance de pacote por segundo (PPS): cada instância do EC2 tem uma performance máxima de PPS, com base no tipo e no tamanho da instância.
- Conexões rastreadas: o grupo de segurança rastreia cada conexão estabelecida para garantir que os pacotes de retorno sejam entregues como esperado. Há um número máximo de conexões que podem ser rastreadas por instância.
- Acesso ao serviço de link local: o Amazon EC2 fornece um PPS máximo por interface de rede para tráfego a serviços, como o serviço de DNS, o serviço de metadados da instância e o Amazon Time Sync Service.

Quando o tráfego de rede de uma instância excede um máximo, a AWS formata o tráfego que excede o máximo ao enfileirar e eliminar pacotes de rede. Você pode monitorar quando o tráfego excede um máximo usando as métricas de performance de rede. Essas métricas informam sobre o impacto no tráfego da rede e possíveis problemas de performance da rede, em tempo real.

Tópicos

- [Requirements \(p. 1042\)](#)
- [Métricas para o driver ENA \(p. 1042\)](#)
- [Exibir as métricas de performance de rede para sua instância do Windows \(p. 1043\)](#)

Requirements

- Instalar o driver ENA versão 2.2.2 ou posterior. Para verificar a versão instalada, use o Gerenciador de dispositivos da seguinte forma.
 1. Abra o Gerenciador de dispositivos executando `devmgmt.msc`.
 2. Expanda Network Adapters (Adaptadores de rede).
 3. Escolha Amazon Elastic Network Adapter , Properties (Propriedades).
 4. Na guia Driver, localize Driver Version (Versão do driver).

Para atualizar seu driver ENA, consulte [Redes avançadas \(p. 1029\)](#).

- Para importar essas métricas para o Amazon CloudWatch, instale o agente CloudWatch. Para obter mais informações, consulte [Coletar métricas avançadas de rede](#) no Guia do usuário do Amazon CloudWatch.

Métricas para o driver ENA

O driver ENA entrega as seguintes métricas para a instância em tempo real. Elas fornecem o número cumulativo de pacotes na fila ou descartados em cada interface de rede desde a última restauração do driver.

Métrica	Descrição
bw_in_allowance_exceeded	Número de pacotes na fila ou descartados porque a largura de banda agregada de entrada excedeu o máximo para a instância.
bw_out_allowance_exceeded	Número de pacotes na fila ou descartados porque a largura de banda agregada de saída excedeu o máximo para a instância.
conntrack_allowance_exceeded	Número de pacotes descartados porque o monitoramento da conexão excedeu o máximo para a instância e não foi possível estabelecer novas conexões. Isso pode resultar em perda de pacotes para tráfego indo para a instância ou vindo da instância
linklocal_allowance_exceeded	Número de pacotes descartados porque o PPS do tráfego para os serviços de proxy local excedeu o máximo para a interface da rede. Isso afeta o tráfego para o serviço de DNS, o Instance Metadata Service e o Amazon Time Sync Service.
pps_allowance_exceeded	Número de pacotes na fila ou descartados porque o PPS bidirecional excedeu o máximo para a instância.

Exibir as métricas de performance de rede para sua instância do Windows

Você pode visualizar as métricas usando qualquer consumidor de contadores de performance do Windows. Os dados podem ser analisados de acordo com o manifesto EnaperfCounters. Esse é um arquivo XML que define o provedor do contador de performance e seus countersets.

Instalação do manifesto

Se você executou a instância usando uma AMI que contém o driver ENA 2.2.2 ou posterior ou usou o script de instalação no pacote de driver para o driver ENA 2.2.2, o manifesto já está instalado. Para instalar o manifesto manualmente, siga as seguintes etapas:

1. Remova o manifesto existente usando o seguinte comando:

```
unlodctr /m:EnaPerfCounters.man
```

2. Copie o arquivo `_EnaPerfCounters.man_` do pacote de instalação do driver para `%SystemRoot%\System32\drivers`.
3. Instale o novo manifesto usando o seguinte comando:

```
lodctr /m:EnaPerfCounters.man
```

Exibir métricas usando o Monitor de performance

1. Abra o Monitor de performance.
2. Pressione Ctrl+N para adicionar novos contadores.
3. Escolha ENA Packets Shaping (Modelagem de pacotes de ENA na lista.

4. Selecione as instâncias a serem monitoradas e escolha Add (Adicionar).
5. Escolha OK.

Grupos de posicionamento

Ao executar uma nova instância do EC2, o serviço do EC2 tenta posicionar a instância de forma que todas as suas instâncias estejam distribuídas pelo hardware subjacente para minimizar falhas correlacionadas. É possível usar placement groups para influenciar o posicionamento de um grupo de instâncias interdependentes para atender às necessidades de sua workload. Dependendo do tipo de workload, você pode criar um placement group com uma das seguintes estratégias de posicionamento:

- Cluster – agrupa instâncias em uma zona de disponibilidade. Essa estratégia permite que as workloads atinjam a performance de rede de baixa latência necessária para a comunicação de nó a nó totalmente acoplada que é típica das aplicações HPC.
- Partição – distribui instâncias entre partições lógicas, de tal modo que instâncias em uma partição não compartilhem o hardware subjacente com grupos de instâncias em diferentes partições. Essa estratégia é normalmente usada por grandes workloads distribuídas e replicadas, como Hadoop, Cassandra e Kafka.
- Disseminar – posiciona estritamente um pequeno grupo de instâncias por hardware subjacente distinto a fim de reduzir falhas correlacionadas.

Não há custo para a criação de um placement group.

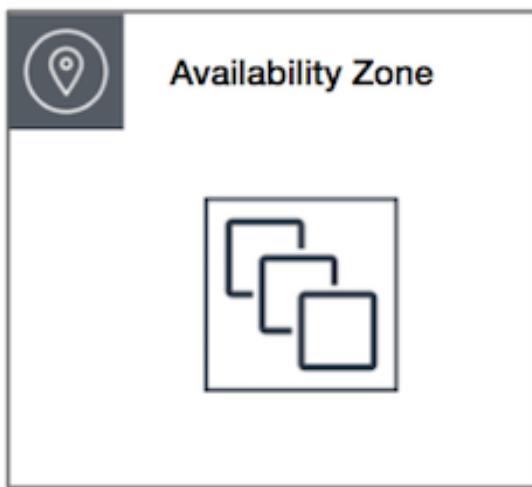
Tópicos

- [Placement groups de cluster \(p. 1044\)](#)
- [Placement groups de partição \(p. 1045\)](#)
- [Placement groups de distribuição \(p. 1046\)](#)
- [Regras e limitações do placement group \(p. 1047\)](#)
- [Criar um placement group. \(p. 1048\)](#)
- [Marcar um placement group \(p. 1049\)](#)
- [Executar instâncias em um placement group \(p. 1051\)](#)
- [Descrever instâncias em um placement group \(p. 1052\)](#)
- [Alterar o placement group de uma instância \(p. 1054\)](#)
- [Excluir um placement group. \(p. 1055\)](#)

Placement groups de cluster

Um placement group de cluster é um agrupamento lógico de instâncias dentro de uma única zona de disponibilidade. Um placement group de cluster pode abranger VPCs emparelhadas na mesma região. As instâncias no mesmo placement group de cluster dispõem de um limite de taxa de transferência por fluxo superior para tráfego TCP/IP e são colocadas no mesmo segmento de largura de banda de bisseção alta da rede.

A imagem a seguir mostra instâncias colocadas em um placement group de cluster.



Os placement groups de cluster são recomendados para aplicações que se beneficiam de baixa latência de rede, alta taxa de transferência de rede ou ambos. Eles também são recomendados quando a maioria do tráfego de rede está entre as instâncias no grupo. Para fornecer a menor latência possível e a melhor performance de rede de pacote por segundo para seu placement group, escolha um tipo de instância que comporte rede avançada. Para obter mais informações, consulte [Redes aprimoradas \(p. 1028\)](#).

Recomendamos executar suas instâncias da seguinte maneira:

- Use uma única solicitação de execução para executar o número de instâncias necessárias no placement group.
- Use o mesmo tipo de instância para todas as instâncias no placement group.

Se você tentar adicionar mais instâncias ao placement group depois ou se tentar executar mais de um tipo de instância no placement group, aumentará as possibilidades de ocorrer um erro de capacidade insuficiente.

Se você interrompe uma instância em um placement group e depois a inicia novamente, ela ainda é executada no placement group. Contudo, ocorrerá uma falha na inicialização se não houver capacidade suficiente para a instância.

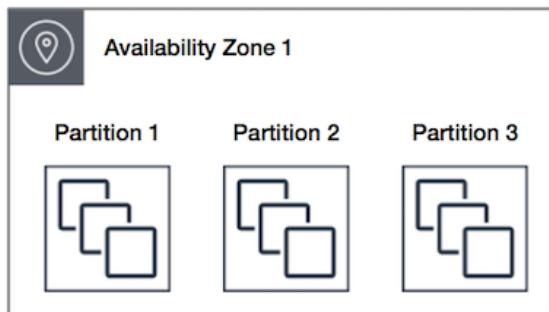
Se você receber um erro de capacidade ao executar uma instância em um placement group que já tenha instâncias em execução, interrompa e inicie todas as instâncias no placement group e tente executá-lo novamente. Iniciar as instâncias pode migrá-las para o hardware com capacidade para todas as instâncias solicitadas.

Placement groups de partição

Os placement groups de partição ajudam a reduzir a probabilidade de falhas de hardware correlacionadas da aplicação. Ao usar grupos de posicionamento de partição, o Amazon EC2 divide cada grupo em segmentos lógicos chamados de partições. O Amazon EC2 garante que cada partição em um grupo de posicionamento tenha seu próprio conjunto de racks. Cada rack tem sua própria rede e fonte de energia. Não há duas partições em um placement group que compartilhem os mesmos racks, permitindo que você isole o impacto da falha de hardware na aplicação.

A imagem a seguir é uma representação visual simples de um placement group de partição em uma única zona de disponibilidade. Ela mostra instâncias que são colocadas em um placement group de partição com três partições — Partition 1 (Partição 1), Partition 2 (Partição 2) e Partition 3 (Partição 3). Cada partição é

composta por várias instâncias. As instâncias em cada partição não compartilham racks com as instâncias nas outras partições, contendo o impacto de uma única falha de hardware apenas na partição associada.



Placement groups de partição podem ser usados para implantar grandes workloads distribuídas e replicadas, como HDFS, HBase e Cassandra, em racks distintos. Ao executar instâncias em um placement group de partição, o Amazon EC2 tenta distribuir as instâncias uniformemente pelo número de partições especificado por você. Também é possível executar instâncias em uma partição específica para ter mais controle sobre onde as instâncias são colocadas.

Um placement group de partição pode ter partições em várias zonas de disponibilidade na mesma região. Um placement group de partição pode ter, no máximo, sete partições por zona de disponibilidade. O número de instâncias que podem ser executadas em um placement group de partição é limitado somente pelos limites da sua conta.

Além disso, placement groups de partição oferecem visibilidade nas partições — é possível ver quais instâncias estão em quais partições. Você pode compartilhar essas informações com aplicações que reconhecem a topologia, como HDFS, HBase e Cassandra. Essas aplicações usam essas informações para tomar decisões inteligentes de replicação de dados para aumentar a disponibilidade e a durabilidade dos dados.

Se você iniciar ou executar uma instância em um placement group de partição e não houver uma quantidade suficiente de hardware exclusivo para atender à solicitação, ocorrerá uma falha. O Amazon EC2 disponibiliza mais hardware distinto ao longo do tempo, portanto, tente reenviar sua solicitação mais tarde.

Placement groups de distribuição

Um placement group de distribuição é um grupo de instâncias que são colocadas cada uma em racks distintos, sendo que cada rack tem sua própria rede e fonte de energia.

A imagem a seguir mostra sete instâncias em uma única zona de disponibilidade que são colocadas em um placement group de distribuição. As sete instâncias são colocadas em sete racks diferentes.



Os placement groups de distribuição são recomendados para aplicativos com uma pequena quantidade de instâncias críticas que devem ser mantidas separadasumas das outras. Executar instâncias em um placement group de distribuição reduz o risco de falhas simultâneas que podem ocorrer quando as instâncias compartilham os mesmos racks. Os placement groups de distribuição concedem acesso a racks distintos e, portanto, são adequados para combinar tipos de instâncias ou executar instâncias ao longo do tempo.

Um placement group de distribuição pode abranger várias zonas de disponibilidade na mesma região. Você pode ter no máximo sete instâncias em execução por zona de disponibilidade por grupo.

Se você iniciar ou executar uma instância em um grupo de posicionamento disseminado e não houver uma quantidade suficiente de hardware exclusivo para atender à solicitação, ocorrerá uma falha. O Amazon EC2 disponibiliza mais hardware distinto ao longo do tempo, portanto, tente reenviar sua solicitação mais tarde.

Regras e limitações do placement group

Regras e limitações gerais

Antes de usar os placement groups, esteja ciente das seguintes regras:

- O nome especificado para um placement group deve ser exclusivo na conta da AWS para a região em questão.
- Não é possível mesclar placement groups.
- Uma instância pode ser executada em um placement group por vez; ela não pode abranger vários placement groups.
- O [Reservas de capacidade sob demanda \(p. 392\)](#) e as [Instâncias reservadas de zona \(p. 262\)](#) fornecem uma reserva de capacidade para instâncias do EC2 em uma zona de disponibilidade específica. A reserva de capacidade pode ser usada por instâncias em um placement group. Contudo, não é possível reservar explicitamente a capacidade de um placement group.
- Não é possível iniciar o Hosts dedicados em placement groups.

Regras e limitações do placement group de cluster

As seguintes regras se aplicam aos placement groups de cluster:

- Somente os seguintes tipos de instância são compatíveis com o no :
 - Instâncias da [geração atual \(p. 150\)](#), exceto as instâncias [expansíveis \(p. 169\)](#) (por exemplo, T2) .
 - As seguintes instâncias da [geração anterior \(p. 152\)](#): A1, C3, cc2.8xlarge, cr1.8xlarge, G2, hs1.8xlarge, I2 e R3.
- Um placement group de cluster não pode abranger várias zonas de disponibilidade.
- A velocidade máxima de taxa de transferência de rede do tráfego entre duas instâncias em um placement group de cluster é limitada pela instância mais lenta. Para aplicações com requisitos de taxa de transferência alta, escolha um tipo de instância com conectividade de rede que atenda a suas necessidades.
- Para instâncias ativadas para a rede avançada, as seguintes regras se aplicam:
 - As instâncias dentro de um placement group de cluster podem usar até 10 Gbps para tráfego de fluxo único. As instâncias que não estiverem dentro de um placement group de cluster poderão usar até 5 Gbps para tráfego de fluxo único.
 - O tráfego para e de buckets do Amazon S3 dentro da mesma região pelo espaço de endereço IP público ou por um VPC endpoint pode usar toda a largura de banda agregada da instância disponível.
- Você pode executar vários tipos de instâncias em um placement group de cluster. No entanto, isso reduz a probabilidade de a capacidade necessária estar disponível para que a execução seja realizada com sucesso. Recomendamos usar o mesmo tipo de instância para todas as instâncias em um placement group de cluster.
- O tráfego de rede para a Internet e por uma conexão da AWS Direct Connect para recursos no local é limitado a 5 Gbps.

Regras e limitações do placement group de partição

As seguintes regras se aplicam aos placement groups de partição:

- Um placement group de partição oferece suporte a, no máximo, sete partições por zona de disponibilidade. O número de instâncias que podem ser executadas em um placement group de partição é limitado somente pelos limites da sua conta.
- Quando as instâncias são executadas em um grupo de posicionamento de partição, o Amazon EC2 tenta distribuir as instâncias uniformemente em todas as partições. O Amazon EC2 não garante uma distribuição uniforme de instâncias em todas as partições.
- Um placement group de partição com Instâncias dedicadas pode ter, no máximo, duas partições.

Regras e limitações do placement group de distribuição

As seguintes regras se aplicam aos placement groups de distribuição:

- Um placement group de distribuição suporta, no máximo, sete instâncias em execução por zona de disponibilidade. Por exemplo, em uma região com três zonas de disponibilidade, você pode executar um total de 21 instâncias no grupo (sete por zona). Se você tentar iniciar uma oitava instância na mesma zona de disponibilidade e no mesmo placement group de distribuição, ela não será executada. Se você precisa de mais de sete instâncias em uma zona de disponibilidade, recomendamos usar vários placement groups de distribuição. O uso de vários placement groups de dispersão não fornece garantias sobre a disseminação de instâncias entre grupos, mas garante a dispersão para cada grupo, limitando assim o impacto de certas classes de falhas.
- Os placement groups de distribuição não são compatíveis com o Instâncias dedicadas.

Criar um placement group.

É possível criar um placement group usando um dos métodos a seguir.

Note

Você pode marcar um placement group na criação usando apenas as ferramentas de linha de comando.

New console

Para criar um placement group usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Placement Groups e Create placement group (Criar placement group).
3. Especifique um nome para o grupo.
4. Escolha a estratégia de posicionamento para o grupo. Se você escolher Partition (Partição), selecione o número de partições no grupo.
5. Escolha Create group (Criar grupo).

Old console

Para criar um placement group usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Placement Groups e Create Placement Group.

3. Especifique um nome para o grupo.
4. Escolha a estratégia de posicionamento para o grupo. Se você escolher Partition (Partição), especifique o número de partições no grupo.
5. Escolha Create (Criar).

AWS CLI

Como criar um placement group usando a AWS CLI

Use o comando [create-placement-group](#). O exemplo a seguir cria um placement group chamado `my-cluster` que usa a estratégia de colocação do `cluster` e aplica uma tag com uma chave de `purpose` e um valor de `production`.

```
aws ec2 create-placement-group --group-name my-cluster --strategy cluster --tag-specifications 'ResourceType=placement-group,Tags=[{Key=purpose,Value=production}]'
```

Como criar um placement group de partição usando a AWS CLI

Use o comando [create-placement-group](#). Especifique o parâmetro `--strategy` com o valor `partition` e especifique o parâmetro `--partition-count` com o número desejado de partições. Neste exemplo, o placement group de partição é chamado de `HDFS-Group-A` e criado com cinco partições.

```
aws ec2 create-placement-group --group-name HDFS-Group-A --strategy partition --partition-count 5
```

PowerShell

Como criar um placement group usando a AWS Tools for Windows PowerShell

Use o comando [New-EC2PlacementGroup](#).

Marcar um placement group

Para categorizar e gerenciar placement groups existentes, você pode marcá-los com metadados personalizados. Para obter mais informações sobre como as tags funcionam, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

Quando você marca um placement group, as instâncias executadas no placement group não são marcadas automaticamente. É necessário marcar explicitamente as instâncias que são executadas no placement group. Para obter mais informações, consulte [Adicionar uma tag ao executar uma instância \(p. 1562\)](#).

Você pode exibir, adicionar e excluir tags usando o novo console e as ferramentas da linha de comando.

New console

Como exibir, adicionar ou excluir uma tag para um placement group existente

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Placement Groups.
3. Selecione um placement group e escolha Actions (Ações), Manage tags (Gerenciar tags).
4. A seção Manage tags (Gerenciar tags) exibe todas as tags atribuídas ao placement group. Para adicionar ou remover tags, siga estas etapas:

- Para adicionar uma tag, escolha Add tag (Adicionar tag), e insira a chave e o valor da tag. Você pode adicionar até 50 tags por placement group. Para obter mais informações, consulte [Restrições de tags \(p. 1558\)](#).
 - Para excluir uma tag, escolha Remove (Remover) ao lado da tag que você deseja excluir.
5. Selecione Save changes (Salvar alterações).

AWS CLI

Como exibir tags de placement group

Use o comando [describe-tags](#) para exibir as tags para o recurso especificado. No exemplo a seguir, descreva as tags para todos os placement groups.

```
aws ec2 describe-tags \
--filters Name=resource-type,Values=placement-group
```

```
{
  "Tags": [
    {
      "Key": "Environment",
      "ResourceId": "pg-0123456789EXAMPLE",
      "ResourceType": "placement-group",
      "Value": "Production"
    },
    {
      "Key": "Environment",
      "ResourceId": "pg-9876543210EXAMPLE",
      "ResourceType": "placement-group",
      "Value": "Production"
    }
  ]
}
```

Você também pode usar o comando [describe-tags](#) para visualizar as tags de um placement group especificando seu ID. No exemplo a seguir, descreva as tags para pg-0123456789EXAMPLE.

```
aws ec2 describe-tags \
--filters Name=resource-id,Values=pg-0123456789EXAMPLE
```

```
{
  "Tags": [
    {
      "Key": "Environment",
      "ResourceId": "pg-0123456789EXAMPLE",
      "ResourceType": "placement-group",
      "Value": "Production"
    }
  ]
}
```

Você também pode exibir as tags de um placement group descrevendo o placement group.

Use o comando [describe-placement-groups](#) para exibir a configuração do placement group especificado, que inclui todas as tags especificadas para o placement group.

```
aws ec2 describe-placement-groups \
--group-name my-cluster
```

```
{  
    "PlacementGroups": [  
        {  
            "GroupName": "my-cluster",  
            "State": "available",  
            "Strategy": "cluster",  
            "GroupId": "pg-0123456789EXAMPLE",  
            "Tags": [  
                {  
                    "Key": "Environment",  
                    "Value": "Production"  
                }  
            ]  
        }  
    ]  
}
```

Como marcar um placement group existente usando o comando da AWS CLI

Você pode usar o comando [create-tags](#) para marcar os recursos existentes. No exemplo a seguir, o placement group existente é marcado com Key=Cost-Center e Value=CC-123.

```
aws ec2 create-tags \  
    --resources pg-0123456789EXAMPLE \  
    --tags Key=Cost-Center,Value=CC-123
```

Como excluir a tag de um placement group usando o comando da AWS CLI

Você pode usar o comando [delete-tags](#) para excluir tags de recursos existentes. Para obter exemplos, consulte [Examples \(Exemplos\)](#) na AWS CLI Command Reference (Referência de comandos da AWS CLI).

PowerShell

Como exibir tags de placement group

Use o comando [Get-EC2Tag](#).

Como descrever as tags de um placement group específico

Use o comando [Get-EC2PlacementGroup](#).

Como marcar um placement group existente

Use o comando [New-EC2Tag](#).

Como excluir a tag de um placement group

Use o comando [Remove-EC2Tag](#).

Executar instâncias em um placement group

É possível executar uma instância em um placement group se as [regras e limitações do placement group forem atendidas \(p. 1047\)](#) usando um dos métodos a seguir.

Console

Para executar instâncias em um placement group usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha Instances (Instâncias).
3. Escolha Launch Instance (Executar instância). Conclua o assistente conforme direcionado, tendo o cuidado de fazer o seguinte:
 - Na página Choose an Instance Type, selecione um tipo de instância que possa ser executado em um placement group.
 - Na página Configure Instance Details (Configurar detalhes da instância), os campos a seguir serão aplicáveis aos placement groups:
 - Em Number of instances (Número de instâncias), insira o número total de instâncias que serão necessárias nesse placement group, pois talvez você não possa adicionar instâncias ao placement group posteriormente.
 - Em Placement group, marque a caixa de seleção Add instance to placement group (Adicionar instância ao placement group). Se Placement group não for exibido nessa página, verifique se você selecionou um tipo de instância que possa ser executado em um placement group. Caso contrário, essa opção não estará disponível.
 - Em Placement group name (Nome do placement group), é possível optar por adicionar as instâncias a um placement group existente ou a um novo placement group que você criar.
 - Em Placement group strategy (Estratégia do placement group), escolha a estratégia apropriada. Se você escolher partition (partição), para Target partition (Destino partição), escolha Auto distribution (Distribuição automática) para que o Amazon EC2 faça o melhor esforço para distribuir as instâncias uniformemente em todas as partições do grupo. Como alternativa, especifique a partição na qual executar as instâncias.

AWS CLI

Como executar instâncias em um placement group usando a AWS CLI

Use o comando [run-instances](#) e especifique o nome do placement group usando o parâmetro `--placement "GroupName = my-cluster"`. Neste exemplo, o placement group é chamado de `my-cluster`.

```
aws ec2 run-instances --placement "GroupName = my-cluster"
```

Como executar instâncias em uma partição específica de um placement group de partição usando a AWS CLI

Use o comando [run-instances](#) e especifique a partição e o nome do placement group usando o parâmetro `--placement "GroupName = HDFS-Group-A, PartitionNumber = 3"`. Neste exemplo, o placement group de partição é chamado de `HDFS-Group-A` e o número de partição é 3.

```
aws ec2 run-instances --placement "GroupName = HDFS-Group-A, PartitionNumber = 3"
```

PowerShell

Como executar instâncias em um placement group usando o AWS Tools for Windows PowerShell

Use o comando [New-EC2Instance](#) e especifique o nome do placement group usando o parâmetro `-Placement_GroupName`.

Descrever instâncias em um placement group

É possível exibir as informações de posicionamento de suas instâncias usando um dos métodos a seguir. Você também pode filtrar placement groups de partição pelo número de partição usando a AWS CLI.

New console

Como exibir o placement group e o número de partição de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Description (Descrição), em Host and placement group (Host e placement group), localize Placement group. Se a instância não estiver em um placement group, o campo estará vazio. Caso contrário, ela conterá o nome do placement group. Se o placement group for um placement group de partição, o Partition number (Número de partição) conterá o número de partição da instância.

Old console

Como exibir o placement group e o número de partição de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Description (Descrição), localize Placement group. Se a instância não estiver em um placement group, o campo estará vazio. Caso contrário, ela conterá o nome do placement group. Se o placement group for um placement group de partição, o Partition number (Número de partição) conterá o número de partição da instância.

AWS CLI

Como visualizar o número da partição para uma instância em um placement group de partição usando a AWS CLI

Use o comando `describe-instances` e especifique o parâmetro `--instance-id`.

```
aws ec2 describe-instances --instance-id i-0123a456700123456
```

A resposta contém as informações de posicionamento, o que inclui o nome do placement group e o número da partição da instância.

```
"Placement": {  
    "AvailabilityZone": "us-east-1c",  
    "GroupName": "HDFS-Group-A",  
    "PartitionNumber": 3,  
    "Tenancy": "default"  
}
```

Como filtrar instâncias para um placement group de partição e número de partição específicos usando a AWS CLI

Use o comando `describe-instances` e especifique o parâmetro `--filters` com os filtros `placement-group-name` e `placement-partition-number`. Neste exemplo, o placement group de partição é chamado de `HDFS-Group-A` e o número de partição é 7.

```
aws ec2 describe-instances --filters "Name = placement-group-name, Values = HDFS-Group-A" "Name = placement-partition-number, Values = 7"
```

A resposta lista todas as instâncias que estão na partição especificada dentro do placement group especificado. A seguir está um exemplo de saída mostrando somente o ID da instância, o tipo de instância e informações de posicionamento das instâncias retornadas.

```
"Instances": [
    {
        "InstanceId": "i-0a1bc23d4567e8f90",
        "InstanceType": "r4.large",
    },
    {
        "Placement": {
            "AvailabilityZone": "us-east-1c",
            "GroupName": "HDFS-Group-A",
            "PartitionNumber": 7,
            "Tenancy": "default"
        }
    },
    {
        "InstanceId": "i-0a9b876cd5d4ef321",
        "InstanceType": "r4.large",
    },
    {
        "Placement": {
            "AvailabilityZone": "us-east-1c",
            "GroupName": "HDFS-Group-A",
            "PartitionNumber": 7,
            "Tenancy": "default"
        }
    }
],
```

Alterar o placement group de uma instância

É possível alterar o placement group de uma instância de qualquer uma das seguintes maneiras:

- Mova uma instância existente para um placement group
- Mova uma instância de um placement group para outro
- Remova uma instância de um placement group

Antes de mover ou remover a instância, ela deve estar no estado `stopped`. É possível mover ou remover uma instância usando a AWS CLI ou um AWS SDK.

AWS CLI

Como mover uma instância para um placement group usando o AWS CLI

1. Interrompa a instância usando o comando [stop-instances](#).
2. Use o comando [modify-instance-placement](#) e especifique o nome do placement group para o qual mover a instância.

```
aws ec2 modify-instance-placement --instance-id i-0123a456700123456 --group-name MySpreadGroup
```

3. Inicie a instância usando o comando [start-instances](#).

PowerShell

Como mover uma instância para um placement group usando o AWS Tools for Windows PowerShell

1. Interrompa a instância usando o comando [Stop-EC2Instance](#).

2. Use o comando [Edit-EC2InstancePlacement](#) e especifique o nome do placement group para o qual mover a instância.
3. Inicie a instância usando o comando [Start-EC2Instance](#).

AWS CLI

Como remover uma instância de um placement group usando o AWS CLI

1. Interrompa a instância usando o comando [stop-instances](#).
2. Use o comando [modify-instance-placement](#) e especifique uma string vazia para o nome do placement group.

```
aws ec2 modify-instance-placement --instance-id i-0123a456700123456 --group-name ""
```

3. Inicie a instância usando o comando [start-instances](#).

PowerShell

Como remover uma instância de um placement group usando o AWS Tools for Windows PowerShell

1. Interrompa a instância usando o comando [Stop-EC2Instance](#).
2. Use o comando [Edit-EC2InstancePlacement](#) e especifique uma string vazia para o nome do placement group.
3. Inicie a instância usando o comando [Start-EC2Instance](#).

Excluir um placement group.

Se precisar substituir um placement group ou se não precisar mais dele, você poderá excluí-lo. É possível excluir um placement group usando um dos métodos a seguir.

Requirement

Para excluir um placement group, ele não deve conter instâncias. É possível [encerrar \(p. 475\)](#) todas as instâncias executadas no placement group, [movê-las \(p. 1054\)](#) para outro placement group ou [removê-las \(p. 1055\)](#) do placement group.

New console

Para excluir um placement group usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Placement Groups.
3. Selecione o placement group e escolha Actions (Ações), Delete (Excluir).
4. Quando a confirmação for solicitada, insira **Delete** e escolha Delete (Excluir).

Old console

Para excluir um placement group usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Placement Groups.

3. Selecione o placement group e escolha Actions (Ações), Delete Placement Group (Excluir placement group).
4. Quando a confirmação for solicitada, escolha Excluir.

AWS CLI

Como excluir um placement group usando o AWS CLI

Use o comando [delete-placement-group](#) e especifique o nome do placement group para excluí-lo. Neste exemplo, o nome do placement group é `my-cluster`.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Como excluir um placement group usando o AWS Tools for Windows PowerShell

Use o comando [Remove-EC2PlacementGroup](#) para excluir o placement group.

Unidade de transmissão máxima (MTU) de rede para a instância do EC2

A unidade de transmissão máxima (MTU) de uma conexão de rede é o tamanho, em bytes, do maior pacote permitível que pode ser passado pela conexão. Quanto maior a MTU de uma conexão, mais dados podem ser passados em um único pacote. Os pacotes de ethernet consistem no quadro, ou nos dados em si que você envia, e nas informações de overhead de rede que o cercam.

Os quadros de ethernet podem vir em diferentes formatos, sendo o mais comum o Ethernet v2 padrão. Ele é compatível com 1.500 MTU, que é o maior tamanho de pacote de Ethernet compatível na maior parte da Internet. A MTU máxima compatível com uma instância depende do tipo de instância. Qualquer tipo de instância do Amazon EC2 é compatível com 1500 MTU e vários tamanhos de instância atuais suportam 9001 MTU ou frames jumbo.

As regras seguintes se aplicam às instâncias que estão em zonas de Wavelength:

- O tráfego que vai de uma instância para outra dentro de uma VPC na mesma zona do Wavelength tem um MTU de 1300.
- O tráfego que vai de uma instância a outra que usa o IP do portador dentro de uma zona de Wavelength tem um MTU de 1500.
- O tráfego que vai de uma instância a outra entre uma zona de Wavelength e a região que usa um endereço IP público tem um MTU de 1500.
- O tráfego que vai de uma instância a outra entre uma zona de Wavelength e a região que usa um endereço IP privado tem um MTU de 1300.

Para ver as informações de MTU de rede para instâncias Linux, alterne para esta página no guia Guia do usuário do Amazon EC2 para instâncias do Linux: [Unidade de transmissão máxima de rede \(MTU\) para sua instância do EC2](#).

Tópicos

- [Frames jumbo \(9.001 MTU\) \(p. 1057\)](#)
- [Path MTU Discovery \(p. 1057\)](#)
- [Verificar o MTU do caminho entre dois hosts \(p. 1058\)](#)
- [Verificar e definir o MTU na instância do Windows \(p. 1058\)](#)

- [Troubleshoot \(p. 1060\)](#)

Frames jumbo (9.001 MTU)

Os frames jumbo permitem mais de 1500 bytes de dados ao aumentar o tamanho da carga útil por pacote, aumentando assim a porcentagem de pacotes que não configura sobrecarga. São necessários menos pacotes para enviar a mesma quantidade de dados usáveis. No entanto, o tráfego é limitado a um MTU máximo de 1500 nos seguintes casos:

- Tráfego fora de um determinado AWS Região para EC2-Classic
- Tráfego fora de uma única VPC
- Tráfego em uma conexão de emparelhamento de VPC entre regiões
- Tráfego através de ligações VPN
- Tráfego em um gateway de Internet

Se os pacotes tiverem mais de 1500 bytes, eles são fragmentados ou caem se o marcador `Don't Fragment` for definido no cabeçalho IP.

Os frames Jumbo devem ser usados com cuidado para o tráfego voltado para Internet ou qualquer tráfego que saia de uma VPC. Os pacotes são fragmentados por sistemas intermediários, que retardam o tráfego. Para usar frames jumbo dentro de uma VPC e não diminuir o tráfego vinculado para fora da VPC, você pode configurar o tamanho de MTU por rota ou usar interfaces de rede elásticas com diferentes tipos de MTU e rotas diferentes.

Para instâncias posicionadas em um placement group de cluster, os frames jumbo ajudam a alcançar a máxima taxa de transferência de rede possível e são recomendados neste caso. Para obter mais informações, consulte [Grupos de posicionamento \(p. 1044\)](#).

Você pode usar quadros jumbo para tráfego entre suas VPCs e suas redes locais por meio do AWS Direct Connect. Para obter mais informações e saber como verificar a capacidade de frames jumbo, consulte [Setting Network MTU \(Configuração de MTU de rede\)](#) no AWS Direct Connect User Guide (Manual do usuário do AWS Direct Connect).

Todas as [instâncias de geração atual \(p. 156\)](#) são compatíveis com quadros jumbo. As seguintes instâncias da geração anterior oferecem suporte a frames jumbo: A1, C3, G2, I2, M3 e R3.

Para obter mais informações sobre tamanhos de MTU compatíveis com gateways de trânsito, consulte [MTU](#) no Gateways de trânsito da Amazon VPC.

Path MTU Discovery

O Path MTU Discovery é usado para determinar o MTU do caminho entre dois dispositivos. O MTU do caminho é o tamanho de pacote máximo suportado no caminho entre o host de origem e o host de recepção.

Para o IPv4, quando um host enviar um pacote que for maior que a MTU do host de recebimento ou que a MTU de um dispositivo ao longo do caminho, o host ou o dispositivo de recebimento eliminará o pacote e retornará a seguinte mensagem ICMP: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Tipo 3, Código 4). Isso instrui o host de transmissão a dividir a carga útil em vários pacotes menores e, em seguida, retransmiti-los.

O protocolo IPv6 não é compatível com a fragmentação na rede. Se um host enviar um pacote que for maior que a MTU do host de recebimento ou que a MTU de um dispositivo ao longo do caminho, o host ou dispositivo de recebimento eliminará o pacote e retornará a seguinte mensagem ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Isso instrui o host de transmissão a dividir a carga útil em vários pacotes menores e, em seguida, retransmiti-los.

Por padrão, os security groups não permitem nenhum tráfego ICMP de entrada. No entanto, os grupos de segurança são stateful, portanto, as respostas ICMP para solicitações de saída têm permissão para fluir, independentemente das regras do grupo de segurança. Portanto, não é necessário adicionar explicitamente uma regra ICMP de entrada para garantir que a instância possa receber a resposta da mensagem ICMP. Para obter mais informações sobre como configurar regras ICMP em uma network ACL, consulte [Descoberta de MTU do caminho](#) no Guia do usuário da Amazon VPC.

Important

O Path MTU Discovery não garante que os quadros Jumbo não sejam descartados por alguns roteadores. Um gateway da Internet na VPC encaminhará somente pacotes de até 1.500 bytes. São recomendados pacotes de 1.500 MTU para o tráfego de Internet.

Verificar o MTU do caminho entre dois hosts

Você pode verificar o MTU do caminho entre dois hosts usando o comando mturoute.exe, , que você pode baixar e instalar de <http://www.elifulkerson.com/projects/mturoute.php>.

Para verificar o MTU o caminho usando mturoute.exe

1. Faça download do mturoute.exe de <http://www.elifulkerson.com/projects/mturoute.php>.
2. Abra uma janela do prompt de comando e altere para o diretório para onde você fez o download de mturoute.exe.
3. Use o comando a seguir para verificar o MTU do caminho entre sua instância do EC2; e outro host. Você pode usar um nome DNS ou um endereço IP como destino. Se o destino for outra instância do EC2, verifique se o security group permite tráfego UDP de entrada. Esse exemplo verifica o MTU do caminho entre a instância do EC2 e a www.elifulkerson.com.

```
.\mturoute.exe www.elifulkerson.com
* ICMP Fragmentation is not permitted. *
* Speed optimization is enabled. *
* Maximum payload is 10000 bytes. *
+ ICMP payload of 1472 bytes succeeded.
- ICMP payload of 1473 bytes is too big.
Path MTU: 1500 bytes.
```

Neste exemplo, o MTU do caminho é 1500.

Verificar e definir o MTU na instância do Windows

Alguns drivers são configurados para usar frames jumbo, e outros são configurados para usar tamanhos de quadro padrão. Convém usar frames jumbo para o tráfego de rede na VPC ou usar quadros padrão para o tráfego da Internet. Seja qual for o seu caso de uso, recomendamos que você verifique se suas instâncias se comportam como esperado.

Se a instância for executada em uma zona de Wavelength, o valor máximo de MTU será 1300.

Driver ENA

Para as versões 1.5 e anteriores do driver

Você pode alterar a configuração do MTU usando o Gerenciador de Dispositivos ou o comando Set-NetAdapterAdvancedProperty.

Para obter a configuração atual do MTU usando o comando Get-NetAdapterAdvancedProperty, use o seguinte comando. Verifique entrada do nome da interface MTU. Um valor de 9001 indica que os frames jumbo estão ativados. Os frames jumbo ficam desativados por padrão.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Ative os frames jumbo da seguinte forma:

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -RegistryValue 9001
```

Desative os frames jumbo da seguinte forma:

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -RegistryValue 1500
```

Para as versões 2.1.0 e posteriores do driver

Você pode alterar a configuração do MTU usando o Gerenciador de Dispositivos ou o comando Set-NetAdapterAdvancedProperty.

Para obter a configuração atual do MTU usando o comando Get-NetAdapterAdvancedProperty, use o seguinte comando. Verifique entrada do nome da interface *JumboPacket. Um valor de 9015 indica que os frames jumbo estão ativados. Os frames jumbo ficam desativados por padrão.

Execute Get-NetAdapterAdvancedProperty ou use curinga (asterisco) para detectar todos os nomes Ethernet correspondentes.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Execute os seguintes comandos e inclua o nome da Ethernet que você deseja consultar.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Ative os frames jumbo da seguinte forma.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -  
RegistryValue 9015
```

Desative os frames jumbo da seguinte forma:

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -  
RegistryValue 1514
```

Driver do Intel SRIOV 82599

Você pode alterar a configuração do MTU usando o Gerenciador de Dispositivos ou o comando Set-NetAdapterAdvancedProperty.

Para obter a configuração atual do MTU usando o comando Get-NetAdapterAdvancedProperty, use o seguinte comando. Verifique entrada do nome da interface *JumboPacket. Um valor de 9014 indica que os frames jumbo estão ativados. (Observe que o tamanho do MTU inclui o cabeçalho e a carga.) Os frames jumbo ficam desativados por padrão.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Ative os frames jumbo da seguinte forma:

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -  
RegistryValue 9014
```

Desative os frames jumbo da seguinte forma:

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -  
RegistryValue 1514
```

AWSDriver PV

Você não pode alterar a configuração do MTU usando o Gerenciador de dispositivos, mas pode alterá-la usando o comando netsh.

Obtenha a configuração atual do MTU usando o seguinte comando. O nome da interface pode variar. Na saída, procure uma entrada intitulada "Ethernet", "Ethernet 2" ou "Conexão Local". Você precisará do nome da interface para ativar ou desativar os frames jumbo. Um valor de 9001 indica que os frames jumbo estão ativados.

```
netsh interface ipv4 show subinterface
```

Ative os frames jumbo da seguinte forma:

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Desative os frames jumbo da seguinte forma:

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Troubleshoot

Se você experimentar problemas de conectividade entre sua instância do EC2 e um cluster do Amazon Redshift ao usar quadros jumbo, consulte [As consultas parecem ficar suspensas](#) no Amazon Redshift Cluster Management Guide

Nuvens privadas virtuais

O Amazon Virtual Private Cloud (Amazon VPC) permite definir uma rede virtual em sua própria área isolada logicamente na Nuvem AWS, conhecida como uma Virtual Private Cloud (VPC). Inicie os recursos da Amazon EC2, como as instâncias, nas sub-redes da VPC. Sua VPC assemelha-se a uma rede tradicional que você poderia operar no seu próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS. Você pode configurar seu VPC, selecionar o intervalo de endereços IP dele, criar sub-redes e definir tabelas de rotas, gateways de rede e configurações de segurança. É possível conectar instâncias na VPC à Internet ou ao seu próprio datacenter.

Quando você cria sua conta da AWS, nós criamos uma VPC padrão para você em cada região. Uma VPC padrão é uma VPC que já está configurada e pronta para uso. Você pode executar instâncias em sua VPC padrão imediatamente. Como alternativa, você pode criar sua própria VPC não padrão e configurá-la, conforme necessário.

Caso você tenha criado sua conta da AWS antes de 4/12/2013, talvez ela seja compatível com a plataforma EC2-Classic em algumas regiões. Se você criou sua conta da AWS depois de 04/12/2013, ela não será compatível com o EC2-Classic e os recursos deverão ser iniciados em uma VPC. Para obter mais informações, consulte [EC2-Classic \(p. 1099\)](#).

Documentação da Amazon VPC

Para obter mais informações sobre uma Amazon VPC, consulte a seguinte documentação.

Guia	Descrição
Manual do usuário da Amazon VPC	Descreve os principais conceitos e disponibiliza instruções para uso dos recursos do Amazon VPC.
Amazon VPC Peering Guide	Descreve as conexões pares da VPC e disponibiliza instruções para usá-las.
Gateways de trânsito da Amazon VPC	Descreve gateways de trânsito e fornece instruções para configura-los e usá-los.
AWS Site-to-Site VPN Guia do usuário	Descreve conexões do Site-to-Site VPN e fornece instruções para configura-las e usá-las.

Portas e protocolos para imagens de máquina da Amazon (AMIs) do Windows

As tabelas a seguir indicam as portas, os protocolos e as direções por workload para Imagens de máquina da Amazon do Windows.

Tópicos

- [Roteador AllJoyn \(p. 1061\)](#)
- [Cast para dispositivo \(p. 1062\)](#)
- [Redes de núcleos \(p. 1064\)](#)
- [Otimização de entrega \(p. 1088\)](#)
- [Trilha de Diag \(p. 1089\)](#)
- [Servidor de protocolo DIAL \(p. 1089\)](#)
- [Gerenciamento Distributed File System \(DFS\) \(p. 1089\)](#)
- [Compartilhamento de arquivos e impressora \(p. 1090\)](#)
- [Gerenciamento remoto do servidor de arquivos \(p. 1094\)](#)
- [Todos os ICMP v4 \(p. 1094\)](#)
- [Multicast \(p. 1095\)](#)
- [Desktop Remoto \(p. 1095\)](#)
- [Gerenciamento de dispositivos do Windows \(p. 1097\)](#)
- [Gerenciamento remoto de Firewall do Windows \(p. 1098\)](#)
- [Gerenciamento remoto do Windows \(p. 1099\)](#)

Roteador AllJoyn

SO	Rule	Descrição	Porta	Protocolo	Direção
Windows Server 2016	Roteador AllJoyn (entrada de TCP)	Regra de entrada para o tráfego do Roteador AllJoyn [TCP]	Local: 9955 Remoto: qualquer um	TCP	Entrada
Windows Server 2019					

SO	Rule	Descrição	Porta	Protocolo	Direção
	Roteador AllJoyn (saída de TCP)	Regra de saída para o tráfego do Roteador AllJoyn [TCP]	Local: qualquer um Remoto: qualquer um	TCP	Saída
	Roteador AllJoyn (entrada de UDP)	Regra de entrada para o tráfego do Roteador AllJoyn [UDP]	Local: qualquer um Remoto: qualquer um	UDP	Entrada
	Roteador AllJoyn (saída de UDP)	Regra de saída para o tráfego do Roteador AllJoyn [UDP]	Local: qualquer um Remoto: qualquer um	UDP	Saída

Cast para dispositivo

SO	Rule	Descrição	Porta	Protocolo	Direção
Windows Server 2016 Windows Server 2019	Funcionalidade Cast para dispositivo (entrada de qWave-TCP)	Regra de entrada para a funcionalidade Cast para dispositivo a fim de permitir o uso do Quality Windows Audio Video Experience Service. [TCP 2177]	Local: 2177 Remoto: qualquer um	TCP	Entrada
	Funcionalidade Cast para dispositivo (saída de qWave-TCP)	Regra de saída para a funcionalidade Cast para dispositivo a fim de permitir o uso do Quality Windows Audio Video Experience Service. [TCP 2177]	Local: qualquer um Remoto: 2177	TCP	Saída
	Funcionalidade Cast para dispositivo	Regra de entrada para a funcionalidade Cast para	Local: 2177 Remoto: qualquer um	UDP	Entrada

SO	Rule	Descrição	Porta	Protocolo	Direção
	(entrada de qWave-UDP)	dispositivo a fim de permitir o uso do Quality Windows Audio Video Experience Service. [UDP 2177]			
	Funcionalidade Cast para dispositivo (saída de qWave-UDP)	Regra de saída para a funcionalidade Cast para dispositivo a fim de permitir o uso do Quality Windows Audio Video Experience Service. [UDP 2177]	Local: qualquer um Remoto: 2177	UDP	Saída
	Descoberta SSDP de Cast para dispositivo (entrada de UDP)	Regra de entrada para permitir a descoberta de destinos Cast para dispositivo usando SSDP	Local: Ply2Disc Remoto: qualquer um	UDP	Entrada
	Servidor de transmissão de Cast para dispositivo (entrada de transmissão HTTP)	Regra de entrada para o servidor Cast para dispositivo a fim de permitir transmissão usando HTTP. [TCP 10246]	Local: 10246 Remoto: qualquer um	TCP	Entrada
	Servidor de transmissão de Cast para dispositivo (entrada de transmissão RTCP)	Regra de entrada para o servidor Cast para dispositivo a fim de permitir transmissão usando RTSP e RTP. [UDP]	Local: qualquer um Remoto: qualquer um	UDP	Entrada

SO	Rule	Descrição	Porta	Protocolo	Direção
	Servidor de transmissão de Cast para dispositivo (saída de transmissão RTP)	Regra de saída para o servidor Cast para dispositivo a fim de permitir transmissão usando RTSP e RTP. [UDP]	Local: qualquer um Remoto: qualquer um	UDP	Saída
	Servidor de transmissão de Cast para dispositivo (entrada de transmissão RTSP)	Regra de entrada para o servidor Cast para dispositivo a fim de permitir streaming usando RTSP e RTP. [TCP 23554, 23555, 23556]	Local: 235, 542, 355, 523, 556 Remoto: qualquer um	TCP	Entrada
	Eventos UPnP de Cast para dispositivo (entrada de TCP)	Regra de entrada para permitir o recebimento de eventos UPnP de destinos de Cast para dispositivo	Local: 2869 Remoto: qualquer um	TCP	Entrada

Redes de núcleos

Windows Server 2012, 2012 R2, 2016, and 2019

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2012	Destination Unreachable (Destino inacessível) (entrada de ICMPv6)	Mensagens de erro Destination Unreachable (Destino inacessível) são enviadas de qualquer nó percorrido por um pacote que seja incapaz de encaminhá-lo por qualquer motivo, exceto congestionamento.	Local: 68 Remoto: 67	ICMPv6	Entrada
Windows Server 2012 R2					
Windows Server 2016					
Windows Server 2019					

SO	Rule	Definição	Porta	Protocolo	Direção
	Destination Unreachable Fragmentation Needed (Destino inacessível, fragmentação necessária) (entrada de ICMPv4)	Mensagens de erro Destination Unreachable Fragmentation Needed (Destino inacessível, fragmentação necessária) são enviadas de qualquer nó percorrido por um pacote que não consiga encaminhá-lo porque era necessária fragmentação e a opção don't fragment (não fragmentar) estava definida.	Local: 68 Remoto: 67	ICMPv4	Entrada
	Redes de núcleos — DNS (saída de UDP)	Regra de saída para permitir solicitações de DNS. Respostas de DNS com base em solicitações correspondentes a essa regra são permitidas, seja qual for o endereço de origem. Esse comportamento é classificado como mapeamento de origem solta.	Local: qualquer um Remota: 53	UDP	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Dynamic Host Configuration Protocol (entrada de DHCP)	Permite mensagens DHCP (Dynamic Host Configuration Protocol) para configuração automática stateful.	Local: 68 Remoto: 67	UDP	Entrada
	Dynamic Host Configuration Protocol (saída de DHCP)	Permite mensagens DHCP (Dynamic Host Configuration Protocol) para configuração automática stateful.	Local: 68 Remoto: 67	UDP	Saída
	Dynamic Host Configuration Protocol para IPv6 (entrada de DHCPV6)	Permite mensagens DHCPV6 (Dynamic Host Configuration Protocol para IPv6) para configurações stateful e stateless.	Local: 546 Remoto: 547	UDP	Entrada
	Dynamic Host Configuration Protocol para IPv6 (saída de DHCPV6)	Permite mensagens DHCPV6 (Dynamic Host Configuration Protocol para IPv6) para configurações stateful e stateless.	Local: 546 Remoto: 547	UDP	Saída
	Redes de núcleos — política de grupo (saída de LSASS)	Regra de saída para permitir tráfego de LSASS remoto para atualizações da política de grupo.	Local: qualquer um Remoto: qualquer um	TCP	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Redes de núcleos — política de grupo (saída de NP)	Redes de núcleos — política de grupo (saída de NP)	Local: qualquer um Remoto: 445	TCP	Saída
	Redes de núcleos — política de grupo (saída de TCP)	Regra de saída para permitir tráfego de RPC remoto para atualizações da política de grupo.	Local: qualquer um Remoto: qualquer um	TCP	Saída
	Internet Group Management Protocol (entrada de IGMP)	Mensagens de IGMP são enviadas e recebidas por nós para criar, unir e separar grupos multicast.	Local: 68 Remoto: 67	2	Entrada
	Redes de núcleos — Internet Group Management Protocol (saída de IGMP)	Mensagens de IGMP são enviadas e recebidas por nós para criar, unir e separar grupos multicast.	Local: 68 Remoto: 67	2	Saída
	Redes de núcleos — IPHTTPS (entrada de TCP)	Regra de TCP de entrada para permitir que a tecnologia de encapsulamento IPHTTPS forneça conectividade entre proxies e firewalls HTTP.	Local: IPHTTPS Remoto: qualquer um	TCP	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Redes de núcleos — IPHTTPS (saída de TCP)	Regra de TCP de saída para permitir que a tecnologia de encapsulamento IPHTTPS forneça conectividade entre proxies e firewalls HTTP.	Local: qualquer um Remoto: IPHTTPS	TCP	Saída
	IPv6 (entrada de IPv6)	Regra de entrada necessária para permitir o tráfego de IPv6 para ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) e serviços de encapsulamento 6to4.	Local: qualquer um Remoto: 445	41	Entrada
	IPv6 (saída de IPv6)	Regra de saída necessária para permitir o tráfego de IPv6 para ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) e serviços de encapsulamento 6to4.	Local: qualquer um Remoto: 445	41	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Multicast Listener Done (Ouvinte multicast concluído) (entrada de ICMPv6)	Mensagens Multicast Listener Done (Ouvinte multicast concluído) informam aos roteadores locais que não há mais membros restantes para um endereço multicast específico nessa sub-rede.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Multicast Listener Done (Ouvinte multicast concluído) (saída de ICMPv6)	Mensagens Multicast Listener Done (Ouvinte multicast concluído) informam aos roteadores locais que não há mais membros restantes para um endereço multicast específico nessa sub-rede.	Local: 68 Remoto: 67	ICMPv6	Saída
	Multicast Listener Query (Consulta do ouvinte multicast) (entrada de ICMPv6)	Um roteador habilitado para multicast IPv6 usa a mensagem Multicast Listener Query (Consulta do ouvinte multicast) a fim de consultar um link para associação de grupo multicast.	Local: 68 Remoto: 67	ICMPv6	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Multicast Listener Query (Consulta do ouvinte multicast) (saída de ICMPv6)	Um roteador habilitado para multicast IPv6 usa a mensagem Multicast Listener Query (Consulta do ouvinte multicast) a fim de consultar um link para associação de grupo multicast.	Local: 68 Remoto: 67	ICMPv6	Saída
	Multicast Listener Report (Relatório do ouvinte multicast) (entrada de ICMPv6)	A mensagem Multicast Listener Report (Relatório do ouvinte multicast) é usada por um nó de escuta para relatar imediatamente seu interesse em receber tráfego multicast em um endereço multicast específico ou em resposta a uma Multicast Listener Query (Consulta do ouvinte multicast).	Local: 68 Remoto: 67	ICMPv6	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Multicast Listener Report (Relatório do ouvinte multicast) (saída de ICMPv6)	A mensagem Multicast Listener Report (Relatório do ouvinte multicast) é usada por um nó de escuta para relatar imediatamente seu interesse em receber tráfego multicast em um endereço multicast específico ou em resposta a uma Multicast Listener Query (Consulta do ouvinte multicast).	Local: 68 Remoto: 67	ICMPv6	Saída
	Multicast Listener Report v2 (Relatório do ouvinte multicast v2) (entrada de ICMPv6)	A mensagem Multicast Listener Report v2 (Relatório do ouvinte multicast v2) é usada por um nó de escuta para relatar imediatamente seu interesse em receber tráfego multicast em um endereço multicast específico ou em resposta a uma Multicast Listener Query (Consulta do ouvinte multicast).	Local: 68 Remoto: 67	ICMPv6	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Multicast Listener Report v2 (Relatório do ouvinte multicast v2) (saída de ICMPv6)	A mensagem Multicast Listener Report v2 (Relatório do ouvinte multicast v2) é usada por um nó de escuta para relatar imediatamente seu interesse em receber tráfego multicast em um endereço multicast específico ou em resposta a uma Multicast Listener Query (Consulta do ouvinte multicast).	Local: 68 Remoto: 67	ICMPv6	Saída
	Neighbor Discovery Advertisement (Anúncio de descoberta de vizinho) (entrada de ICMPv6)	Mensagens Neighbor Discovery Advertisement (Anúncio de descoberta de vizinho) são enviadas por nós para notificar outros nós de alterações no endereço de camada de link ou em resposta a uma solicitação Neighbor Discovery Solicitation (Solicitação de descoberta de vizinho).	Local: 68 Remoto: 67	ICMPv6	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Neighbor Discovery Advertisement (Anúncio de descoberta de vizinho) (saída de ICMPv6)	Mensagens Neighbor Discovery Advertisement (Anúncio de descoberta de vizinho) são enviadas por nós para notificar outros nós de alterações no endereço de camada de link ou em resposta a uma solicitação Neighbor Discovery Solicitation (Solicitação de descoberta de vizinho).	Local: 68 Remoto: 67	ICMPv6	Saída
	Neighbor Discovery Solicitation (Solicitação de descoberta de vizinho) (entrada de ICMPv6)	Neighbor Discovery Solicitations (Solicitações de descoberta de vizinho) são enviadas por nós para descobrir o endereço de camada de link de outro nó IPv6 no link.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Neighbor Discovery Solicitation (Solicitação de descoberta de vizinho) (saída de ICMPv6)	Neighbor Discovery Solicitations (Solicitações de descoberta de vizinho) são enviadas por nós para descobrir o endereço de camada de link de outro nó IPv6 no link.	Local: 68 Remoto: 67	ICMPv6	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Packet Too Big (Pacote muito grande) (entrada de ICMPv6)	Mensagens de erro Packet Too Big (Pacote muito grande) são enviadas de qualquer nó percorrido por um pacote que seja incapaz de encaminhá-lo porque o pacote é grande demais para o próximo link.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Packet Too Big (Pacote muito grande) (saída de ICMPv6)	Mensagens de erro Packet Too Big (Pacote muito grande) são enviadas de qualquer nó percorrido por um pacote que seja incapaz de encaminhá-lo porque o pacote é grande demais para o próximo link.	Local: 68 Remoto: 67	ICMPv6	Saída
	Parameter Problem (Problema de parâmetro) (entrada de ICMPv6)	Mensagens de erro Parameter Problem (Problema de parâmetro) são enviadas por nós quando os pacotes são gerados incorretamente.	Local: 68 Remoto: 67	ICMPv6	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Parameter Problem (Problema de parâmetro) (saída de ICMPv6)	Mensagens de erro Parameter Problem (Problema de parâmetro) são enviadas por nós quando os pacotes são gerados incorretamente.	Local: 68 Remoto: 67	ICMPv6	Saída
	Router Advertisement (Anúncio do roteador) (entrada de ICMPv6)	Mensagens Router Advertisement (Anúncio do roteador) são enviadas por roteadores a outros nós para configuração automática stateless.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Router Advertisement (Anúncio do roteador) (saída de ICMPv6)	Mensagens Router Advertisement (Anúncio do roteador) são enviadas por roteadores a outros nós para configuração automática stateless.	Local: 68 Remoto: 67	ICMPv6	Saída
	Router Solicitation (Solicitação do roteador) (entrada de ICMPv6)	Mensagens Router Solicitation (Solicitação do roteador) são enviadas por nós que buscam roteadores para fornecer configuração automática stateless.	Local: 68 Remoto: 67	ICMPv6	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Router Solicitation (Solicitação do roteador) (saída de ICMPv6)	Mensagens Router Solicitation (Solicitação do roteador) são enviadas por nós que buscam roteadores para fornecer configuração automática stateless.	Local: 68 Remoto: 67	ICMPv6	Saída
	Redes de núcleos — Teredo (entrada de UDP)	Regra de UDP de entrada para permitir o percurso de borda Teredo. Essa técnologia fornec atribuição de endereço e encapsulamento automático para o tráfego IPv6 unicast quando um host IPv6/IPv4 está localizado atrás de um conversor de endereços de rede IPv4.	Local: Teredo Remoto: qualquer um	UDP	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Redes de núcleos — Teredo (saída de UDP)	Regra de UDP de saída para permitir o percurso de borda Teredo. Essa tecnologia fornece atribuição de endereço e encapsulamento automático para o tráfego IPv6 unicast quando um host IPv6/IPv4 está localizado atrás de um conversor de endereços de rede IPv4.	Local: qualquer um Remoto: qualquer um	UDP	Saída
	Time Exceeded (Tempo excedido) (entrada de ICMPv6)	Mensagens de erro Time Exceeded (Tempo excedido) são geradas de qualquer nó percorrido por um pacote se o valor Hop Limit (Limite de salto) é reduzido para zero em qualquer ponto do caminho.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Time Exceeded (Tempo excedido) (saída de ICMPv6)	Mensagens de erro Time Exceeded (Tempo excedido) são geradas de qualquer nó percorrido por um pacote se o valor Hop Limit (Limite de salto) é reduzido para zero em qualquer ponto do caminho.	Local: 68 Remoto: 67	ICMPv6	Saída

Windows Server 2008 R2 and SP2

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2008 R2 Windows Server 2008 SP2	Destination Unreachable (Destino inacessível) (entrada de ICMPv6)	Mensagens de erro Destination Unreachable (Destino inacessível) são enviadas de qualquer nó percorrido por um pacote que seja incapaz de encaminhá-lo por qualquer motivo, exceto congestionamento.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Destination Unreachable Fragmentation Needed (Destino inacessível, fragmentação necessária) (entrada de ICMPv4)	Mensagens de erro Destination Unreachable Fragmentation Needed (Destino inacessível, fragmentação necessária) são enviadas de qualquer nó percorrido por um pacote que não consiga encaminhá-lo porque era necessária fragmentação e a opção don't fragment (não fragmentar) estava definida.	Local: 68 Remoto: 67	ICMPv4	Entrada
	Dynamic Host Configuration Protocol (entrada de DHCP)	Permite mensagens DHCP (Dynamic Host Configuration Protocol) para configuração automática stateful.	Local: 68 Remoto: 67	UDP	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Dynamic Host Configuration Protocol (saída de DHCP)	Permite mensagens DHCP (Dynamic Host Configuration Protocol) para configuração automática stateful.	Local: 68 Remoto: 67	UDP	Saída
	Dynamic Host Configuration Protocol para IPv6 (entrada de DHCPV6)	Permite mensagens DHCPV6 (Dynamic Host Configuration Protocol para IPv6) para configurações stateful e stateless.	Local: 546 Remoto: 547	UDP	Entrada
	Dynamic Host Configuration Protocol para IPv6 (saída de DHCPV6)	Permite mensagens DHCPV6 (Dynamic Host Configuration Protocol para IPv6) para configurações stateful e stateless.	Local: 546 Remoto: 547	UDP	Saída
	Internet Group Management Protocol (entrada de IGMP)	Mensagens de IGMP são enviadas e recebidas por nós para criar, unir e separar grupos multicast.	Local: 68 Remoto: 67	2	Entrada
	IPv6 (entrada de IPv6)	Regra de entrada necessária para permitir o tráfego de IPv6 para ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) e serviços de encapsulamento 6to4.	Local: qualquer um Remoto: 445	41	Entrada

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Redes de núcleos

SO	Rule	Definição	Porta	Protocolo	Direção
	IPv6 (saída de IPv6)	Regra de saída necessária para permitir o tráfego de IPv6 para ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) e serviços de encapsulamento 6to4.	Local: qualquer um Remoto: 445	41	Saída
	Multicast Listener Done (Ouvinte multicast concluído) (entrada de ICMPv6)	Mensagens Multicast Listener Done (Ouvinte multicast concluído) informam aos roteadores locais que não há mais membros restantes para um endereço multicast específico nessa sub-rede.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Multicast Listener Done (Ouvinte multicast concluído) (saída de ICMPv6)	Mensagens Multicast Listener Done (Ouvinte multicast concluído) informam aos roteadores locais que não há mais membros restantes para um endereço multicast específico nessa sub-rede.	Local: 68 Remoto: 67	ICMPv6	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Multicast Listener Query (Consulta do ouvinte multicast) (entrada de ICMPv6)	Um roteador habilitado para multicast IPv6 usa a mensagem Multicast Listener Query (Consulta do ouvinte multicast) a fim de consultar um link para associação de grupo multicast.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Multicast Listener Query (Consulta do ouvinte multicast) (saída de ICMPv6)	Um roteador habilitado para multicast IPv6 usa a mensagem Multicast Listener Query (Consulta do ouvinte multicast) a fim de consultar um link para associação de grupo multicast.	Local: 68 Remoto: 67	ICMPv6	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Multicast Listener Report (Relatório do ouvinte multicast) (entrada de ICMPv6)	A mensagem Multicast Listener Report (Relatório do ouvinte multicast) é usada por um nó de escuta para relatar imediatamente seu interesse em receber tráfego multicast em um endereço multicast específico ou em resposta a uma Multicast Listener Query (Consulta do ouvinte multicast).	Local: 68 Remoto: 67	ICMPv6	Entrada
	Multicast Listener Report (Relatório do ouvinte multicast) (saída de ICMPv6)	A mensagem Multicast Listener Report (Relatório do ouvinte multicast) é usada por um nó de escuta para relatar imediatamente seu interesse em receber tráfego multicast em um endereço multicast específico ou em resposta a uma Multicast Listener Query (Consulta do ouvinte multicast).	Local: 68 Remoto: 67	ICMPv6	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Multicast Listener Report v2 (Relatório do ouvinte multicast v2) (entrada de ICMPv6)	A mensagem Multicast Listener Report v2 (Relatório do ouvinte multicast v2) é usada por um nó de escuta para relatar imediatamente seu interesse em receber tráfego multicast em um endereço multicast específico ou em resposta a uma Multicast Listener Query (Consulta do ouvinte multicast).	Local: 68 Remoto: 67	ICMPv6	Entrada
	Multicast Listener Report v2 (Relatório do ouvinte multicast v2) (saída de ICMPv6)	A mensagem Multicast Listener Report v2 (Relatório do ouvinte multicast v2) é usada por um nó de escuta para relatar imediatamente seu interesse em receber tráfego multicast em um endereço multicast específico ou em resposta a uma Multicast Listener Query (Consulta do ouvinte multicast).	Local: 68 Remoto: 67	ICMPv6	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Neighbor Discovery Advertisement (Anúncio de descoberta de vizinho) (entrada de ICMPv6)	Mensagens Neighbor Discovery Advertisement (Anúncio de descoberta de vizinho) são enviadas por nós para notificar outros nós de alterações no endereço de camada de link ou em resposta a uma solicitação Neighbor Discovery Solicitation (Solicitação de descoberta de vizinho).	Local: 68 Remoto: 67	ICMPv6	Entrada
	Neighbor Discovery Advertisement (Anúncio de descoberta de vizinho) (saída de ICMPv6)	Mensagens Neighbor Discovery Advertisement (Anúncio de descoberta de vizinho) são enviadas por nós para notificar outros nós de alterações no endereço de camada de link ou em resposta a uma solicitação Neighbor Discovery Solicitation (Solicitação de descoberta de vizinho).	Local: 68 Remoto: 67	ICMPv6	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Neighbor Discovery Solicitation (Solicitação de descoberta de vizinho) (entrada de ICMPv6)	Neighbor Discovery Solicitations (Solicitações de descoberta de vizinho) são enviadas por nós para descobrir o endereço de camada de link de outro nó IPv6 no link.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Neighbor Discovery Solicitation (Solicitação de descoberta de vizinho) (saída de ICMPv6)	Neighbor Discovery Solicitations (Solicitações de descoberta de vizinho) são enviadas por nós para descobrir o endereço de camada de link de outro nó IPv6 no link.	Local: 68 Remoto: 67	ICMPv6	Saída
	Packet Too Big (Pacote muito grande) (entrada de ICMPv6)	Mensagens de erro Packet Too Big (Pacote muito grande) são enviadas de qualquer nó percorrido por um pacote que seja incapaz de encaminhá-lo porque o pacote é grande demais para o próximo link.	Local: 68 Remoto: 67	ICMPv6	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Packet Too Big (Pacote muito grande) (saída de ICMPv6)	Mensagens de erro Packet Too Big (Pacote muito grande) são enviadas de qualquer nó percorrido por um pacote que seja incapaz de encaminhá-lo porque o pacote é grande demais para o próximo link.	Local: 68 Remoto: 67	ICMPv6	Saída
	Parameter Problem (Problema de parâmetro) (entrada de ICMPv6)	Mensagens de erro Parameter Problem (Problema de parâmetro) são enviadas por nós quando os pacotes são gerados incorretamente.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Parameter Problem (Problema de parâmetro) (saída de ICMPv6)	Mensagens de erro Parameter Problem (Problema de parâmetro) são enviadas por nós quando os pacotes são gerados incorretamente.	Local: 68 Remoto: 67	ICMPv6	Saída
	Router Advertisement (Anúncio do roteador) (entrada de ICMPv6)	Mensagens Router Advertisement (Anúncio do roteador) são enviadas por roteadores a outros nós para configuração automática stateless.	Local: 68 Remoto: 67	ICMPv6	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Router Advertisement (Anúncio do roteador) (saída de ICMPv6)	Mensagens Router Advertisement (Anúncio do roteador) são enviadas por roteadores a outros nós para configuração automática stateless.	Local: 68 Remoto: 67	ICMPv6	Saída
	Router Solicitation (Solicitação do roteador) (entrada de ICMPv6)	Mensagens Router Solicitation (Solicitação do roteador) são enviadas por nós que buscam roteadores para fornecer configuração automática stateless.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Router Solicitation (Solicitação do roteador) (saída de ICMPv6)	Mensagens Router Solicitation (Solicitação do roteador) são enviadas por nós que buscam roteadores para fornecer configuração automática stateless.	Local: 68 Remoto: 67	ICMPv6	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Time Exceeded (Tempo excedido) (entrada de ICMPv6)	Mensagens de erro Time Exceeded (Tempo excedido) são geradas de qualquer nó percorrido por um pacote se o valor Hop Limit (Limite de salto) é reduzido para zero em qualquer ponto do caminho.	Local: 68 Remoto: 67	ICMPv6	Entrada
	Time Exceeded (Tempo excedido) (saída de ICMPv6)	Mensagens de erro Time Exceeded (Tempo excedido) são geradas de qualquer nó percorrido por um pacote se o valor Hop Limit (Limite de salto) é reduzido para zero em qualquer ponto do caminho.	Local: 68 Remoto: 67	ICMPv6	Saída

Otimização de entrega

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2019	Entrada de DeliveryOptimization TCP	Regra de Entrada para permitir que a Otimização de entrega se conecte a endpoints remotos.	Local: 7680 Remoto: qualquer um	TCP	Entrada
	Entrada de DeliveryOptimization UDP	Regra de Entrada para permitir que a Otimização de entrega se conecte	Local: 7680 Remoto: qualquer um	UDP	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
		a endpoints remotos.			

Trilha de Diag

Windows Server 2019

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2019	Telemetria e experiências do usuário conectado	Tráfego de saída do cliente de telemetria unificada	Local: qualquer um Remoto: 443	TCP	Saída

Windows Server 2016

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2016	Telemetria e experiências do usuário conectado	Tráfego de saída do cliente de telemetria unificada	Local: qualquer um Remoto: qualquer um	TCP	Saída

Servidor de protocolo DIAL

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2016 Windows Server 2019	Servidor de protocolo DIAL (entrada de HTTP)	Regra de entrada para o servidor de protocolo DIAL a fim de permitir o controle remoto de aplicações que usam HTTP.	Local: 10247 Remoto: qualquer um	TCP	Entrada

Gerenciamento Distributed File System (DFS)

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2008 R2	Gerenciamento DFS (entrada de SMB)	Regra de entrada para permitir que	Local: 445	TCP	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
		o tráfego de SMB gerencie a função File Services (Serviços de arquivo).	Remoto: qualquer um		
	Gerenciamento DFS (entrada de WMI)	Regra de entrada para permitir que o tráfego de WMI gerencie a função File Services (Serviços de arquivo).	Local: RPC Remoto: qualquer um	TCP	Entrada
	Gerenciamento DFS (entrada de DCOM)	Regra de entrada para permitir que o tráfego de DCOM gerencie a função File Services (Serviços de arquivo).	Local: 135 Remoto: qualquer um	TCP	Entrada
	Gerenciamento DFS (entrada de TCP)	Regra de entrada para permitir que o tráfego de TCP gerencie a função File Services (Serviços de arquivo).	Local: RPC Remoto: qualquer um	TCP	Entrada

Compartilhamento de arquivos e impressora

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2008 R2	Compartilhamento de arquivos e impressora (Echo Request (Solicitação Echo) — entrada de ICMPv4)	Mensagens Echo Request (Solicitação Echo) são enviadas como solicitações ping para outros nós.	Local: 5355 Remoto: qualquer um	ICMPv4	Entrada
Windows Server 2008 SP2					
Windows Server 2012					
Windows Server 2012 R2	Compartilhamento de arquivos e impressora	Mensagens Echo Request (Solicitação	Local: 5355	ICMPv4	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	(Echo Request (Solicitação Echo) — saída de ICMPv4)	Echo) são enviadas como solicitações ping para outros nós.	Remoto: qualquer um		
	Compartilhamento de arquivos e impressora (Echo Request (Solicitação Echo) — entrada de ICMPv6)	Mensagens Echo Request (Solicitação Echo) são enviadas como solicitações ping para outros nós.	Local: 5355 Remoto: qualquer um	ICMPv6	Entrada
	Compartilhamento de arquivos e impressora (Echo Request (Solicitação Echo) — saída de ICMPv6)	Mensagens Echo Request (Solicitação Echo) são enviadas como solicitações ping para outros nós.	Local: 5355 Remoto: qualquer um	ICMPv6	Saída
	Compartilhamento de arquivos e impressora (entrada de LLMNR-UDP)	Regra de entrada para compartilhamento de arquivos e impressora a fim de permitir a Resolução de nomes multicast de local de link.	Local: 5355 Remoto: qualquer um	UDP	Entrada
	Compartilhamento de arquivos e impressora (saída de LLMNR-UDP)	Regra de saída para compartilhamento de arquivos e impressora a fim de permitir a Resolução de nomes multicast de local de link.	Local: qualquer um Remoto: 5355	UDP	Saída
	Compartilhamento de arquivos e impressora (entrada de NB-Datagram)	Regra de entrada para o compartilhamento de arquivos e impressora a fim de permitir a transmissão e a recepção de datagramas do NetBIOS.	Local: 138 Remoto: qualquer um	UDP	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Compartilhamento de arquivos e impressora (saída de NB-Datagram)	Regra de saída para o compartilhamento de arquivos e impressora a fim de permitir a transmissão e a recepção de datagramas do NetBIOS.	Local: qualquer um Remoto: 138	UDP	Saída
	Compartilhamento de arquivos e impressora (entrada de NB-Name)	Regra de entrada para o compartilhamento de arquivos e impressora a fim de permitir a Resolução de nomes do NetBIOS.	Local: 137 Remoto: qualquer um	UDP	Entrada
	Compartilhamento de arquivos e impressora (saída de NB-Name)	Regra de saída para o compartilhamento de arquivos e impressora a fim de permitir a Resolução de nomes NetBIOS.	Local: qualquer um Remoto: 137	UDP	Saída
	Compartilhamento de arquivos e impressora (entrada de NB-Session)	Regra de entrada para o compartilhamento de arquivos e impressora a fim de permitir conexões do serviço de sessões do NetBIOS.	Local: 139 Remoto: qualquer um	TCP	Entrada
	Compartilhamento de arquivos e impressora (saída de NB-Session)	Regra de saída para o compartilhamento de arquivos e impressora a fim de permitir conexões do serviço de sessões do NetBIOS.	Local: qualquer um Remoto: 139	TCP	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
	Compartilhamento de arquivos e impressora (entrada de SMB)	Regra de entrada para o compartilhamento de arquivos e impressora a fim de permitir a transmissão e a recepção de blocos de mensagens do servidor por meio de pipes nomeados.	Local: 445 Remoto: qualquer um	TCP	Entrada
	Compartilhamento de arquivos e impressora (saída de SMB)	Regra de saída para o compartilhamento de arquivos e impressora a fim de permitir a transmissão e a recepção de blocos de mensagens do servidor por meio de pipes nomeados.	Local: qualquer um Remoto: 445	TCP	Saída
	Compartilhamento de arquivos e impressora (serviço de spooler — RPC)	Regra de entrada para o compartilhamento de arquivos e impressora a fim de permitir que o serviço de spooler da impressora se comunique por TCP/RPC.	Local: RPC Remoto: qualquer um	TCP	Entrada
	Compartilhamento de arquivos e impressora (serviço de spooler — RPC — EPMAP)	Regra de entrada para o serviço RPCSS a fim de permitir o tráfego RPC/TCP para o serviço de spooler.	Local: RPC-EPMAP Remoto: qualquer um	TCP	Entrada

Gerenciamento remoto do servidor de arquivos

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2008 SP2 Windows Server 2012 Windows Server 2012 R2	Gerenciamento remoto do servidor de arquivos (entrada de DCOM)	Regra de entrada para permitir que o tráfego de DCOM gerencie a função File Services (Serviços de arquivo).	Local: 135 Remoto: qualquer um	TCP	Entrada
	Gerenciamento remoto do servidor de arquivos (entrada de SMB)	Regra de entrada para permitir que o tráfego de SMB gerencie a função File Services (Serviços de arquivo).	Local: 445 Remoto: qualquer um	TCP	Entrada
	Entrada de WMI	Regra de entrada para permitir que o tráfego de WMI gerencie a função File Services (Serviços de arquivo).	Local: RPC Remoto: qualquer um	TCP	Entrada

Todos os ICMP v4

SO	Rule	Porta	Protocolo	Direção
Windows Server 2012 Windows Server 2012 R2	Todos os ICMP v4	Local: 139 Remoto: qualquer um	ICMPv4	Entrada

Multicast

Windows Server 2019

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2019	mDNS (entrada de UDP)	Regra de entrada para o tráfego de mDNS.	Local: 5353 Remoto: qualquer um	UDP	Entrada
	mDNS (saída de UDP)	Regra de saída para o tráfego de mDNS.	Local: qualquer um Remoto: 5353	UDP	Saída

Windows Server 2016

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2016	mDNS (entrada de UDP)	Regra de entrada para o tráfego de mDNS.	Local: mDNS Remoto: qualquer um	UDP	Entrada
	mDNS (saída de UDP)	Regra de saída para o tráfego de mDNS.	Local: 5353 Remoto: qualquer um	UDP	Saída

Desktop Remoto

Windows Server 2012 R2, 2016, and 2019

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	Desktop Remoto — sombra (entrada de TCP)	Regra de entrada para o serviço Desktop Remoto a fim de permitir o sombreamento de uma sessão existente do Desktop Remoto	Local: qualquer um Remoto: qualquer um	TCP	Entrada
	Desktop Remoto — modo	Regra de entrada para o serviço	Local: 3389 Remoto: qualquer um	TCP	Entrada

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Desktop Remoto

SO	Rule	Definição	Porta	Protocolo	Direção
	de usuário (entrada de TCP)	Desktop Remoto a fim de permitir o tráfego de RDP.			
	Desktop Remoto — modo de usuário (entrada de UDP)	Regra de entrada para o serviço Desktop Remoto a fim de permitir o tráfego de RDP.	Local: 3389 Remoto: qualquer um	UDP	Entrada

Windows Server 2012

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2012	Desktop Remoto — modo de usuário (entrada de TCP)	Regra de entrada para o serviço Desktop Remoto a fim de permitir o tráfego de RDP.	Local: 3389 Remoto: qualquer um	TCP	Entrada
	Desktop Remoto — modo de usuário (entrada de UDP)	Regra de entrada para o serviço Desktop Remoto a fim de permitir o tráfego de RDP.	Local: 3389 Remoto: qualquer um	UDP	Entrada

Windows Server 2008 SP2

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2008 SP2	Desktop Remoto — sombra (entrada de TCP)	Regra de entrada para o serviço Desktop Remoto a fim de permitir o sombreamento de uma sessão existente do Desktop Remoto	Local: qualquer um Remoto: qualquer um	TCP	Entrada

SO	Rule	Definição	Porta	Protocolo	Direção
	Desktop Remoto — modo de usuário (entrada de TCP)	Regra de entrada para o serviço Desktop Remoto a fim de permitir o tráfego de RDP.	Local: 3389 Remoto: qualquer um	TCP	Entrada
	Desktop Remoto — modo de usuário (entrada de UDP)	Regra de entrada para o serviço Desktop Remoto a fim de permitir o tráfego de RDP.	Local: 3389 Remoto: qualquer um	UDP	Entrada

Windows Server 2008 R2

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2008 R2	RemoteFX (entrada de TCP)	Regra de entrada para o serviço Desktop Remoto a fim de permitir o tráfego de RDP.	Local: 3389 Remoto: qualquer um	TCP	Entrada
	Entrada de TCP	Regra de entrada para o serviço Desktop Remoto a fim de permitir o tráfego de RDP.	Local: 3389 Remoto: qualquer um	TCP	Entrada

Gerenciamento de dispositivos do Windows

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2019	Instalador do certificado de gerenciamento de dispositivos do Windows (saída de TCP)	Permite o tráfego de TCP de saída do Instalador do certificado de gerenciamento	Local: qualquer um Remoto: qualquer um	TCP	Saída

SO	Rule	Definição	Porta	Protocolo	Direção
		de dispositivos do Windows.			
	Serviço de cadastro no gerenciamento de dispositivos do Windows (saída de TCP)	Permite o tráfego de TCP de saída do Serviço de cadastro no gerenciamento de dispositivos do Windows.	Local: qualquer um Remoto: qualquer um	TCP	Saída
	Cliente de sincronização do gerenciamento de dispositivos do Windows (saída de TCP)	Permite o tráfego de TCP de saída do Cliente de sincronização do gerenciamento de dispositivos do Windows.	Local: qualquer um Remoto: qualquer um	TCP	Saída
	WinRT de cadastro do Windows (saída de TCP)	Permite o tráfego de TCP de saída do WinRT de cadastro do Windows.	Local: qualquer um Remoto: qualquer um	TCP	Saída

Gerenciamento remoto de Firewall do Windows

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2008 SP2 Windows Server 2012 R2	Gerenciamento remoto de Firewall do Windows (RPC)	Regra de entrada para que o Firewall do Windows seja gerenciado remotamente por RPC/TCP.	Local: RPC Remoto: qualquer um	TCP	Entrada
	Gerenciamento remoto do Firewall do Windows (RPC-EPMAP)	Regra de entrada para o serviço RPCSS a fim de permitir o tráfego de RPC/TCP para o Firewall do Windows.	Local: RPC-EPMAP Remoto: qualquer um	TCP	Entrada

Gerenciamento remoto do Windows

SO	Rule	Definição	Porta	Protocolo	Direção
Windows Server 2008 R2	Gerenciamento remoto do Windows (entrada de HTTP)	Regra de entrada para o Gerenciamento remoto do Windows pelo WS-Management.	Local: 5985 Remoto: qualquer um	TCP	Entrada
Windows Server 2012					
Windows Server 2012 R2					
Windows Server 2016					
Windows Server 2019					

Para obter mais informações sobre grupos de segurança do Amazon EC2, consulte [Grupos de segurança do Amazon EC2 para instâncias do Windows](#).

EC2-Classic

Com EC2-Classic, suas instâncias executadas em uma única rede simples que você compartilha com outros clientes. Com a Amazon VPC, suas instâncias são executadas em uma nuvem privada virtual (VPC) que é isolada logicamente para a conta da AWS.

A plataforma EC2-Classic foi introduzida na versão original do Amazon EC2. Se você criou a conta da AWS depois de 04/12/2013, ela não será compatível com o EC2-Classic e as instâncias do Amazon EC2 deverão ser iniciadas em uma VPC.

Se sua conta não for compatível com EC2-Classic, criaremos uma VPC para você. Por padrão, quando você executar uma instância, iniciaremos essa instância na VPC padrão. Como alternativa, você pode criar uma VPC não padrão e especificá-la ao executar uma instância.

Detectar plataformas suportadas

O console do Amazon EC2 indica as plataformas nas quais você pode executar instâncias para a região selecionada e se você tem ou não uma VPC padrão nessa região.

Verifique se a região que será usada está selecionada na barra de navegação. No console do painel do Amazon EC2, procure Supported Platforms (Plataformas compatíveis) em Account Attributes (Atributos da conta).

Contas compatíveis com o EC2-Classic

O painel exibe o seguinte em Atributos da conta para indicar que a conta é compatível com a plataforma EC2-Classic e com VPCs nessa região, mas a região não tem uma VPC padrão.

Account Attributes



Supported Platforms

EC2

VPC

A saída do comando `describe-account-attributes` inclui os valores EC2 e VPC do atributo `supported-platforms`.

```
aws ec2 describe-account-attributes --attribute-names supported-platforms
{
    "AccountAttributes": [
        {
            "AttributeName": "supported-platforms",
            "AttributeValues": [
                {
                    "AttributeValue": "EC2"
                },
                {
                    "AttributeValue": "VPC"
                }
            ]
        }
    ]
}
```

Contas que exigem uma VPC

O painel exibe o seguinte em Atributos da conta para indicar que a conta requer uma VPC para executar instâncias nesta região que não é compatível com a plataforma EC2-Classic nessa região, e que a região tem uma VPC padrão com o identificador `vpc-1a2b3c4d`.

Account Attributes



Supported Platforms

VPC

Default VPC

`vpc-1a2b3c4d`

A saída do comando `describe-account-attributes` para a região especificada inclui somente o valor VPC do atributo `supported-platforms`.

```
aws ec2 describe-account-attributes --attribute-names supported-platforms --region us-east-2
{
    "AccountAttributes": [
        {
            "AttributeValues": [
                {
                    "AttributeValue": "VPC"
                }
            ]
        }
    ]
}
```

Tipos de instância disponíveis no EC2-Classic

A maioria dos tipos de instância mais novos requer uma VPC. Os tipos de instância a seguir são os únicos tipos com suporte no EC2-Classic:

- Uso geral: M1, M3 e T1
- Computação otimizada: C1, C3 e CC2
- Memória otimizada: CR1, M2 e R3
- Armazenamento otimizado: D2, HS1 e I2
- Computação acelerada: G2

Se sua conta oferecer suporte ao EC2-Classic, mas você não criou uma VPC não padrão, poderá executar um dos seguintes procedimentos para executar instâncias que requerem uma VPC:

- Crie uma VPC não padrão e execute uma instância somente de VPC nela especificando um ID de sub-rede ou um ID de interface de rede na solicitação. Observe que você deve criar uma VPC não padrão se não tiver uma VPC padrão e estiver usando a AWS CLI, a API do Amazon EC2 ou o AWS SDK para executar uma instância somente de VPC.
- Execute sua instância somente de VPC usando o console do Amazon EC2. O console do Amazon EC2 cria uma VPC não padrão em sua conta e executa a instância na sub-rede na primeira zona de disponibilidade. O console cria a VPC com os seguintes atributos:
 - Uma sub-rede em cada zona de disponibilidade, com o atributo de endereço IPv4 público definido como `true` para que as instâncias recebam um endereço IPv4 público. Para obter mais informações, consulte [Endereço IP em sua VPC](#) no Guia do usuário da Amazon VPC.
 - Um gateway da Internet e uma tabela de rotas principal que roteia o tráfego na VPC para o gateway da Internet. Isso permite que as instâncias executadas na VPC se comuniquem pela Internet. Para obter mais informações, consulte [Gateways da Internet](#) no Guia do usuário da Amazon VPC.
 - Um security group padrão para a VPC e uma network ACL padrão associada a cada sub-rede. Para obter mais informações, consulte [Grupos de segurança para sua VPC](#) no Guia do usuário da Amazon VPC.

Se você tiver outros recursos no EC2-Classic, poderá executar etapas para migrá-los para uma VPC. Para obter mais informações, consulte [Migre do EC2-Classic para uma VPC \(p. 1119\)](#).

Diferenças entre instâncias no EC2-Classic e em uma VPC

A tabela a seguir resume as diferenças entre as instâncias executadas no EC2-Classic, as instâncias executadas em uma VPC padrão e as instâncias executadas em uma VPC não padrão.

Característica	EC2-Classic	VPC padrão	VPC não padrão
Endereço IPv4 público (do grupo de endereços IP públicos da Amazon)	Sua instância recebe um endereço IPv4 público do grupo de endereços IPv4 públicos do EC2-Classic.	A instância executada em uma sub-rede padrão recebe um endereço IPv4 público por padrão, a menos que você especifique o contrário durante a execução ou modifique o atributo de endereço IPv4 público da sub-rede.	Por padrão, a instância não recebe um endereço IPv4 público, a menos que você especifique o contrário durante a execução ou modifique o atributo de endereço IPv4 público da sub-rede.

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Diferenças entre instâncias no EC2-Classic e em uma VPC

Característica	EC2-Classic	VPC padrão	VPC não padrão
		endereço IPv4 público da sub-rede.	
Endereço IPv4 privado	A instância recebe um endereço IPv4 privado do intervalo do EC2-Classic toda vez que é iniciada.	A instância recebe um endereço IPv4 privado estático do intervalo de endereços de sua VPC padrão.	A instância recebe um endereço IPv4 privado estático do intervalo de endereços de sua VPC.
Vários endereços IPv4 privados	Nós selecionamos um único endereço IP privado para sua instância; vários endereços IP não têm suporte.	Você pode atribuir à instância vários endereços IPv4 privados.	Você pode atribuir à instância vários endereços IPv4 privados.
Endereço IP elástico (IPv4)	O IP elástico é desassociado da instância quando você interrompe a instância.	Um IP elástico permanece associado à instância quando você interrompe a instância.	Um IP elástico permanece associado à instância quando você interrompe a instância.
Como associar um endereço IP elástico	Você associa um endereço IP elástico a uma instância.	O endereço IP elástico é uma propriedade de uma interface de rede. Você pode associar um endereço IP elástico a uma instância atualizando a interface de rede anexada à instância.	O endereço IP elástico é uma propriedade de uma interface de rede. Você pode associar um endereço IP elástico a uma instância atualizando a interface de rede anexada à instância.
Como reassociar um endereço IP elástico	Se o endereço IP elástico já estiver associado a outra instância, o endereço será associado automaticamente à nova instância.	Se o endereço IP elástico já estiver associado a outra instância, o endereço será associado automaticamente à nova instância.	Caso o endereço IP elástico já esteja associado a outra instância, será bem-sucedido somente se você tiver permitido uma nova associação.
Marcar endereços IP elásticos	Não é possível aplicar tags a um endereço IP elástico.	Você pode aplicar tags a um endereço IP elástico.	Você pode aplicar tags a um endereço IP elástico.
Nomes de hosts DNS	Por padrão, os nomes de hosts DNS estão ativados.	Por padrão, os nomes de hosts DNS estão ativados.	Por padrão, os nomes de hosts DNS estão desativados.
Grupo de segurança	Um grupo de segurança pode consultar grupos de segurança que pertencem a outras contas da AWS.	Um grupo de segurança pode fazer referência aos grupos de segurança da sua VPC, ou a uma VPC de mesmo nível em uma conexão de emparelhamento de VPC.	Um grupo de segurança só pode consultar security groups de sua VPC.

Característica	EC2-Classic	VPC padrão	VPC não padrão
Associação a grupos de segurança	Não é possível alterar os security groups de uma instância em execução. Você pode modificar as regras dos security groups atribuídos ou substituir a instância por uma nova (crie uma AMI a partir da instância, execute uma nova instância a partir dessa AMI com os security groups necessários, desassocie todos os endereços IP elásticos da instância original, associe-os à nova instância e, em seguida, encerre a instância original).	Você pode atribuir até 5 security groups a uma instância. Você pode atribuir security groups à sua instância ao executá-la e durante sua execução.	Você pode atribuir até 5 security groups a uma instância. Você pode atribuir security groups à sua instância ao executá-la e durante sua execução.
Regras de grupos de segurança	Só é possível adicionar regras para o tráfego de entrada.	É possível adicionar regras para o tráfego de entrada e de saída.	É possível adicionar regras para o tráfego de entrada e de saída.
Locação	Sua instância é executada em hardware compartilhado.	A instância pode ser executada em hardware compartilhado ou em hardware de um único locatário.	A instância pode ser executada em hardware compartilhado ou em hardware de um único locatário.
Como acessar a Internet	Sua instância pode acessar a Internet. Sua instância recebe automaticamente um endereço IP público e pode acessar a Internet diretamente por meio da borda de rede da AWS.	Por padrão, sua instância pode acessar a Internet. Sua instância recebe um endereço IP público por padrão. Um gateway da Internet está anexado à sua VPC padrão, e sua sub-rede padrão tem uma rota para o gateway da Internet.	Por padrão, sua instância não pode acessar a Internet. Sua instância não recebe um endereço IP público por padrão. Sua VPC pode ter um gateway da Internet, dependendo de como foi criada.
Endereços IPv6	Os endereços IPv6 não têm suporte. Você não pode atribuir endereços IPv6 às suas instâncias.	Associe, opcionalmente, um bloco CIDR IPv6 à VPC e atribua endereços IPv6 às instâncias em sua VPC.	Associe, opcionalmente, um bloco CIDR IPv6 à VPC e atribua endereços IPv6 às instâncias em sua VPC.

Grupos de segurança do EC2-Classic

Se estiver usando o EC2-Classic, você deverá usar grupos de segurança criados especificamente para o EC2-Classic. Quando você executa uma instância no EC2-Classic, você deve especificar um grupo de segurança na mesma região que a instância. Você não pode especificar um security group criado para uma VPC quando executa uma instância no EC2-Classic.

Depois de executar uma instância no EC2-Classic, você não pode alterar os security groups. No entanto, você pode adicionar ou remover regras de um security group a qualquer momento, e essas alterações

serão aplicadas automaticamente a todas as instâncias associadas ao security group após um breve período.

Sua conta da AWS tem automaticamente um grupo de segurança padrão por região para o EC2-Classic. Se tentar excluir o grupo de segurança padrão, você receberá o seguinte erro: Client.InvalidGroup.Reserved: o grupo de segurança "padrão" está reservado.

Você pode criar grupos de segurança personalizados. O nome do grupo de segurança deve ser exclusivo dentro da sua conta para a região. Para criar um grupo de segurança para uso no EC2-Classic, escolha No VPC (Sem VPC) para a VPC.

Você pode adicionar regras de entrada para os grupos de segurança padrão e personalizado. Você não pode alterar as regras de saída de um security group do EC2-Classic. Ao criar um grupo de segurança, você pode usar um grupo de segurança diferente para EC2-Classic na mesma região como origem ou destino. Para especificar um grupo de segurança de outra conta da AWS, adicione o ID de conta da AWS como um prefixo; por exemplo, 111122223333/sg-edcd9784.

No EC2-Classic, você pode ter até 500 grupos de segurança em cada região para cada conta. Você pode adicionar até 100 regras ao security group. Você pode ter até 800 regras de grupo de segurança por instância. Isso é calculado como o múltiplo de regras por grupo de segurança e grupos de segurança por instância. Se você fizer referência a outros grupos de segurança nas regras de grupo de segurança, recomendamos que use nomes de grupo de segurança com menos de 22 caracteres.

Endereçamento IP e DNS

A Amazon fornece um servidor DNS que resolve nomes de host DNS IPv4 fornecidos pela Amazon para endereços IPv4. No EC2-Classic, o servidor DNS da Amazon está localizado em 172.16.0.23.

Se você criar uma configuração de firewall personalizada no EC2-Classic, deverá criar uma regra no firewall que permita tráfego de entrada na porta 53 (DNS) — com uma porta de destino do intervalo efêmero — do endereço do servidor DNS da Amazon. Caso contrário, haverá falha na resolução DNS interna de suas instâncias. Se o firewall não permitir respostas a consultas DNS automaticamente, você precisará permitir o tráfego do endereço IP do servidor DNS da Amazon. Para obter o endereço IP do servidor DNS da Amazon, use o seguinte comando na instância:

```
ipconfig /all | findstr /c:"DNS Servers"
```

Endereços IP elásticos

Se sua conta oferecer suporte ao EC2-Classic, haverá um grupo de endereços IP elásticos para uso com a plataforma EC2-Classic e outro para uso com suas VPCs. Não é possível associar um endereço IP elástico que você aloca para uso com uma VPC a uma instância no EC2-Classic e vice-versa. No entanto, você pode migrar um endereço IP elástico alocado para uso na plataforma EC2-Classic para uso com uma VPC. Não é possível migrar um endereço IP elástico para outra região.

Para alocar um endereço IP elástico para uso no EC2-Classic usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Escolha Allocate new address.
4. Selecione Classic e escolha Allocate. Feche a tela de confirmação.

Migrar um endereço IP elástico do EC2-Classic

Se sua conta oferecer suporte ao EC2-Classic, você poderá migrar endereços IP elásticos que alocou para uso com a plataforma EC2-Classic a ser usada com uma VPC, dentro da mesma região. Isso pode ajudar

a migrar seus recursos do EC2-Classic para uma VPC; por exemplo, você pode executar servidores Web novos na VPC, e usar os mesmos endereços IP elásticos que usava para seus servidores Web no EC2-Classic para seus novos servidores Web na VPC.

Depois de migrar um endereço IP elástico para uma VPC, não é possível usá-lo com EC2-Classic. No entanto, você pode restaurá-lo para EC2-Classic se necessário. Não é possível migrar um endereço IP elástico que foi alocado originalmente para uso com uma VPC para o EC2-Classic.

Para migrar um endereço IP elástico, ele não deve estar associado a uma instância. Para obter mais informações sobre como desassociar um endereço IP elástico de uma instância, consulte [Dissociar um endereço IP elástico \(p. 998\)](#).

É possível migrar tantos endereços IP elásticos do EC2-Classic quanto for possível em sua conta. No entanto, ao migrar um endereço IP elástico, ele conta em relação ao limite de endereços IP elásticos de VPCs. Não é possível migrar um endereço IP elástico se, como resultado, seu limite for excedido. De maneira semelhante, quando você restaura um endereço IP elástico para o EC2-Classic, ele conta em relação ao limite de endereços IP elásticos do EC2-Classic. Para obter mais informações, consulte [Limite de endereços IP elásticos \(p. 1001\)](#).

Não é possível migrar um endereço IP elástico que foi alocado a sua conta por menos de 24 horas.

Você pode migrar um endereço IP elástico do EC2-Classic usando o console do Amazon EC2 ou o console da Amazon VPC. Essa opção só estará disponível se a conta oferecer suporte ao EC2-Classic.

Para mover um endereço IP elástico usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico e escolha Actions, Move to VPC scope.
4. Na caixa de diálogo de confirmação, escolha Move Elastic IP.

Você pode restaurar um endereço IP elástico para o EC2-Classic usando o console do Amazon EC2 ou o console da Amazon VPC.

Para restaurar um endereço IP elástico para o EC2-Classic usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic IPs.
3. Selecione o endereço IP elástico e escolha Actions, Restore to EC2 scope.
4. Na caixa de diálogo de confirmação, escolha Restore.

Depois de executar o comando para mover ou restaurar seu endereço IP elástico, o processo de migração do endereço IP elástico pode demorar alguns minutos. Use o comando [describe-moving-addresses](#) para verificar se o endereço IP elástico ainda está sendo movido ou se a movimentação foi concluída.

Depois de mover o endereço IP elástico, você poderá visualizar seu ID de alocação na página Elastic IPs no campo Allocation ID.

Se o endereço IP elástico estiver em um estado de movimentação há mais de cinco minutos, entre em contato com o [Premium Support](#).

Para mover um endereço IP elástico usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [move-address-to-vpc](#) (AWS CLI)

-
- [Move-EC2AddressToVpc](#) (AWS Tools for Windows PowerShell)

Para restaurar um endereço IP elástico para EC2-Classic usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [restore-address-to-classic](#) (AWS CLI)
- [Restore-EC2AddressToClassic](#) (AWS Tools for Windows PowerShell)

Para descrever o status de seus endereços em movimentação usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [describe-moving-addresses](#) (AWS CLI)
- [Get-EC2Address](#) (AWS Tools for Windows PowerShell)

Compartilhar e acessar recursos entre EC2-Classic e uma VPC

Alguns recursos e funcionalidades de sua conta da AWS podem ser compartilhados ou acessados entre o EC2-Classic e uma VPC, por exemplo, por meio do ClassicLink. Para obter mais informações, consulte [ClassicLink \(p. 1107\)](#).

Se sua conta oferece suporte ao EC2-Classic, você pode já ter configurado recursos para usar no EC2-Classic. Se você quiser migrar do EC2-Classic para uma VPC, deverá reciar esses recursos em sua VPC. Para obter mais informações sobre como migrar do EC2-Classic para uma VPC, consulte [Migre do EC2-Classic para uma VPC \(p. 1119\)](#).

Os seguintes recursos podem ser compartilhados ou acessados entre o EC2-Classic e uma VPC.

Recurso	Observações
AMI	
Tarefa de pacote	
Volume do EBS	
Endereço IP elástico (IPv4)	É possível migrar um endereço IP elástico do EC2-Classic para uma VPC. Não é possível migrar um endereço IP elástico que foi alocado originalmente para uso em uma VPC para o EC2-Classic. Para obter mais informações, consulte Migrar um endereço IP elástico do EC2-Classic (p. 1104) .
Instância	Uma instância do EC2-Classic pode se comunicar com instâncias em uma VPC usando endereços IPv4 públicos ou usar o ClassicLink para habilitar a comunicação por endereços IPv4 privados. Não é possível migrar uma instância do EC2-Classic para uma VPC. Contudo, é possível migrar

Recurso	Observações
	sua aplicação de uma instância na EC2-Classic para uma instância em uma VPC. Para obter mais informações, consulte Migre do EC2-Classic para uma VPC (p. 1119) .
Par de chaves	
Load balancer	<p>Se você estiver usando o ClassicLink, poderá registrar uma instância do EC2-Classic vinculada com um load balancer em uma VPC, desde que a VPC tenha uma sub-rede na mesma zona de disponibilidade que a instância.</p> <p>Não é possível migrar um load balancer do EC2-Classic para uma VPC. Você não pode registrar uma instância em uma VPC com um load balancer no EC2-Classic.</p>
Placement group	
Reserved Instance	Você pode alterar a plataforma de rede para Instâncias reservadas do EC2-Classic para uma VPC. Para obter mais informações, consulte Modificar a Instâncias reservadas (p. 289) .
Grupo de segurança	<p>Uma instância do EC2-Classic vinculada pode usar grupos de segurança de VPC pelo ClassicLink para controlar o tráfego para e da VPC. As instâncias de VPC não podem usar security groups do EC2-Classic.</p> <p>Não é possível migrar um security group do EC2-Classic para uma VPC. Você pode copiar regras de um grupo de segurança no EC2-Classic para um grupo de segurança em uma VPC. Para obter mais informações, consulte Crie um grupo de segurança (p. 1223).</p>
Snapshot	

Os seguintes recursos não podem ser compartilhados nem movidos entre o EC2-Classic e uma VPC:

- Spot Instances

ClassicLink

O ClassicLink permite vincular instâncias do EC2-Classic a uma VPC em sua conta, dentro da mesma região. Se você associar os grupos de segurança da VPC à instância do EC2-Classic, isso permite a comunicação entre a instância do EC2-Classic e as instâncias na VPC, usando endereços IPv4 privados. Com o ClassicLink, não há necessidade de usar endereços IPv4 públicos ou endereços IP elásticos para permitir a comunicação entre instâncias nestas plataformas.

O ClassicLink está disponível para todos os usuários com contas que oferecem suporte à plataforma EC2-Classic e pode ser usado com qualquer instância do EC2-Classic. Para obter mais informações sobre como migrar seus recursos para uma VPC, consulte [Migre do EC2-Classic para uma VPC \(p. 1119\)](#).

Não há cobrança adicional pelo uso do ClassicLink. Aplicam-se as cobranças padrão pela transferência de dados e pelo uso de instâncias.

Tópicos

- [Conceitos básicos de ClassicLink \(p. 1108\)](#)
- [Limitações do ClassicLink \(p. 1110\)](#)
- [Trabalhar com ClassicLink \(p. 1111\)](#)
- [Exemplos de políticas do IAM para ClassicLink \(p. 1115\)](#)
- [Exemplo: configuração do grupo de segurança do ClassicLink para uma aplicação Web de três níveis \(p. 1117\)](#)

Conceitos básicos de ClassicLink

Há duas etapas para vincular uma instância do EC2-Classic a uma VPC usando o ClassicLink. Primeiro, você deve habilitar a VPC para ClassicLink. Por padrão, todas VPCs na sua conta não são habilitadas para ClassicLink, para manter o isolamento. Depois de habilitar a VPC para ClassicLink, você poderá vincular qualquer instância do EC2-Classic em execução na mesma região da sua conta a essa VPC. Vincular sua instância inclui selecionar security groups da VPC para associar com sua instância do EC2-Classic. Após ter vinculado a instância, ele pode se comunicar com as instâncias na sua VPC usando seus endereços IP privados, desde que os security groups da VPC permitam. Sua instância do EC2-Classic não perde seu endereço IP privado quando ligada à VPC.

Vincular sua instância a uma VPC às vezes é chamado de associar sua instância.

Uma instância vinculada do EC2-Classic pode se comunicar com instâncias em uma VPC, mas não faz parte da VPC. Se você listar suas instâncias e filtrar por VPC, por exemplo, por meio da solicitação de API `DescribeInstances` ou utilizando a tela Instâncias do console do Amazon EC2, os resultados não retornarão nenhuma instância do EC2-Classic vinculada à VPC. Para obter mais informações sobre visualização das suas instâncias vinculadas do EC2-Classic, consulte [Visualizar suas VPCs habilitadas para ClassicLink e as instâncias vinculadas \(p. 1113\)](#).

Por padrão, se você usar um hostname de DNS público para endereçar uma instância em uma VPC de uma instância vinculada do EC2-Classic, o hostname resolverá para o endereço IP públicos da instância. O mesmo ocorre se você usar um hostname de DNS público para abordar uma instância vinculada do EC2-Classic a partir de uma instância na VPC. Se você quiser que o hostname de DNS público resolva para o endereço IP privado, pode habilitar o suporte a DNS do ClassicLink para VPC. Para obter mais informações, consulte [Habilitar o suporte a DNS do ClassicLink \(p. 1113\)](#).

Se você não precisar mais de uma conexão do ClassicLink entre sua instância e a VPC, pode desvincular a instância do EC2-Classic da VPC. Isso dissocia os security groups da VPC da instância do EC2-Classic. Uma instância vinculada do EC2-Classic é automaticamente desvinculada de uma VPC quando interrompida. Após desvincular todas as instâncias vinculadas do EC2-Classic da VPC, você pode desabilitar o ClassicLink da VPC.

Uso de outros serviços da AWS na sua VPC com o ClassicLink

As instâncias vinculadas do EC2-Classic podem acessar os seguintes serviços da AWS na VPC: Amazon Redshift, Amazon ElastiCache, Elastic Load Balancing e Amazon RDS. No entanto, as instâncias na VPC não podem acessar os serviços da AWS provisionados pela plataforma do EC2-Classic usando o ClassicLink.

Se você usa o Elastic Load Balancing, pode registrar suas instâncias vinculadas do EC2-Classic junto ao load balancer. É necessário criar seu load balancer na VPC habilitada para ClassicLink e ativar a zona de disponibilidade em que a instância é executada. Se você encerrar a instância vinculada do EC2-Classic, o load balancer cancelará o registro da instância.

Se você usar o Amazon EC2 Auto Scaling, poderá criar um grupo do Amazon EC2 Auto Scaling com instâncias automaticamente ligadas a uma VPC habilitada para ClassicLink na execução. Para obter mais informações, consulte [Vínculo de instâncias do EC2-Classic a uma VPC](#) no Guia do usuário do Amazon EC2 Auto Scaling.

Se você usa instâncias de Amazon RDS ou clusters de Amazon Redshift na sua VPC e eles estiverem acessíveis publicamente (acessível pela Internet), o endpoint que você usar para endereçar esses recursos a partir de uma instância vinculada do EC2-Classic por padrão resolverá para um endereço IP público. Se esses recursos não estiverem publicamente acessíveis, o endpoint resolverá para um endereço IP privado. Para endereçar uma instância do RDS publicamente acessível ou um cluster do Redshift sobre IP privado usando o ClassicLink, você deve usar o endereço IP privado ou o hostname privado de DNS, ou então habilitar o suporte a DNS do ClassicLink para a VPC.

Se você usar um hostname de DNS privado ou um endereço IP privado para endereçar uma instância do RDS, a instância vinculada do EC2-Classic não poderá usar o suporte a failover disponível para implantações Multi-AZ.

Você pode usar o console do Amazon EC2 para encontrar os endereços IP privados dos seus recursos Amazon Redshift, Amazon ElastiCache ou Amazon RDS.

Para localizar os endereços IP privados de recursos da AWS na sua VPC

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Network Interfaces.
3. Verifique as descrições das interfaces de rede na coluna Descrição. Uma interface de rede usada em Amazon Redshift, Amazon ElastiCache ou Amazon RDS trará o nome do serviço na descrição. Por exemplo, uma interface de rede anexada a uma instância do Amazon RDS terá a seguinte descrição: **RDSNetworkInterface**.
4. Selecione a interface de rede necessária.
5. No painel de detalhes, obtenha o endereço IP privado do campo Primary private IPv4 IP (IP IPv4 privado primário).

Controlar o uso de ClassicLink

Por padrão, os usuários do IAM não têm permissão para trabalhar com o ClassicLink. Você pode criar uma política do IAM que conceda permissões a usuários para habilitar ou desabilitar uma VPC para ClassicLink, vincular ou desvincular uma instância a uma VPC habilitada para ClassicLink e exibir VPCs habilitadas para ClassicLink e instâncias do EC2-Classic vinculadas. Para obter mais informações sobre políticas do IAM para Amazon EC2, consulte [Políticas do IAM no Amazon EC2 \(p. 1139\)](#).

Para obter mais informações sobre as políticas para trabalhar com ClassicLink, consulte o exemplo a seguir: [Exemplos de políticas do IAM para ClassicLink \(p. 1115\)](#).

Grupos de segurança no ClassicLink

Vincular sua instância do EC2-Classic a uma VPC não afeta seus security groups do EC2-Classic. Eles continuam a controlar todo o tráfego que vai e volta da instância. Isso não inclui o tráfego de e para as instâncias na VPC, que é controlado pelos grupos de segurança da VPC que você associou à instância do EC2-Classic. As instâncias do EC2-Classic que estão vinculadas à mesma VPC não podem se comunicar entre si por meio da VPC; independentemente de estarem associadas ao mesmo grupo de segurança da VPC. Uma comunicação entre as instâncias do EC2-Classic é controlada pelos grupos de segurança do EC2-Classic associados a essas instâncias. Para um exemplo de uma configuração de security group, consulte [Exemplo: configuração do grupo de segurança do ClassicLink para uma aplicação Web de três níveis \(p. 1117\)](#).

Depois de ligar sua instância a uma VPC, você não poderá alterar quais security groups da VPC estão associados à instância. Para associar diferentes security groups à sua instância, primeiro desvincule a instância e depois vincule-a novamente à VPC, escolhendo os security groups necessários.

Roteamento para ClassicLink

Quando você habilita uma VPC para o ClassicLink, é adicionada uma rota estática a todas as tabelas de rotas da VPC com os destinos 10.0.0.0/8 e local. Isso permite a comunicação entre instâncias da VPC e qualquer instância do EC2-Classic que esteja vinculada à VPC. Se adicionar uma tabela de rotas personalizada a uma VPC habilitada para o ClassicLink, será automaticamente adicionada uma rota estática com o destino de 10.0.0.0/8 e alvo de local. Ao desativar o ClassicLink para uma VPC, essa rota será excluída automaticamente de todas as tabelas de rotas da VPC.

As VPCs que estão nos intervalos de endereços IP 10.0.0.0/16 e 10.1.0.0/16 poderão ser habilitadas para o ClassicLink somente se não tiverem nenhuma rota estática existente nas tabelas de rotas do intervalo de endereços IP 10.0.0.0/8, excluindo as rotas locais adicionadas automaticamente quando a VPC foi criada. Da mesma forma, se já tiver habilitado uma VPC para o ClassicLink, pode ser que não consiga adicionar nenhuma rota mais específica às suas tabelas de rotas dentro do intervalo de endereços IP 10.0.0.0/8.

Important

Se o bloco CIDR da VPC for um intervalo de endereços IP publicamente roteável, considere as implicações de segurança antes de vincular uma instância do EC2-Classic à sua VPC. Por exemplo, se sua instância vinculada do EC2-Classic receber uma flood attack de solicitação de negação de serviço (Denial of Service, DoS) de entrada de um endereço IP de origem que se encaixa no intervalo de endereços IP da VPC, o tráfego de resposta será enviado à sua VPC. Nós recomendamos veementemente que você crie sua VPC usando um intervalo de endereços IP privados, como especificado em [RFC 1918](#).

Para obter mais informações sobre as tabelas de rotas e o roteamento em sua VPC, consulte [Tabelas de rotas](#) no Guia do usuário da Amazon VPC.

Habilitar uma conexão de emparelhamento de VPC para ClassicLink

Se você tiver uma conexão de emparelhamento de VPC entre duas VPCs e houver uma ou mais instâncias do EC2-Classic vinculadas a uma ou às duas VPCs por ClassicLink, você poderá ampliar a conexão de emparelhamento de VPC para permitir a comunicação entre as instâncias do EC2-Classic e as instâncias na VPC do outro lado da conexão de emparelhamento de VPC. Isso permite que as instâncias do EC2-Classic e as instâncias na VPC se comuniquem usando endereços IP privados. Para fazer isso, você pode habilitar uma VPC local para se comunicar com uma instância do EC2-Classic vinculada em uma VPC de mesmo nível ou habilitar uma instância do EC2-Classic local vinculada para se comunicar com instâncias VPC em uma VPC de mesmo nível.

Se você habilitar uma VPC local para se comunicar com um EC2-Classic vinculado; em uma VPC de mesmo nível, uma rota estática será adicionada automaticamente às tabelas de rotas com um destino de 10.0.0.0/8 e um alvo de local.

Para obter mais informações e exemplos, consulte [Configurações com ClassicLink](#) no Amazon VPC Peering Guide.

Limitações do ClassicLink

Para usar o recurso ClassicLink, você precisa estar ciente das seguintes limitações:

- Você pode vincular uma instância do EC2-Classic a apenas uma VPC por vez.
- Se você parar sua instância vinculada do EC2-Classic, ela será automaticamente desvinculada da VPC e os security groups da VPC são estarão mais associados à instância. Você pode vincular sua instância à VPC novamente depois de reiniciá-la.
- Você não pode vincular uma instância do EC2-Classic a uma VPC que esteja em uma região diferente ou em uma conta diferente da AWS.

- Você não pode usar o ClassicLink para vincular uma VPC a uma VPC diferente ou um recursos do EC2-Classic. Para estabelecer uma conexão privada entre VPCs, você pode usar uma conexão de VPC do mesmo nível. Para obter mais informações, consulte o [Amazon VPC Peering Guide \(Guia de emparelhamento da Amazon VPC\)](#).
- Não é possível associar um endereço IP elástico da VPC com uma instância do EC2-Classic vinculada.
- Você não pode habilitar instâncias do EC2-Classic para comunicação IPv6. Você pode associar um bloco CIDR de IPv6 com sua VPC e atribuir o endereço IPv6 a recursos na sua VPC, mas a comunicação entre uma instância ClassicLinked e os recursos na VPC é somente sobre IPv4.
- As VPCs com rotas que entram em conflito com a faixa de endereços IP privados do EC2-Classic de 10/8 não podem ser habilitadas para ClassicLink. Isso não inclui VPCs com intervalos de endereço IP 10.0.0.0/16 e 10.1.0.0/16 que já tenham rotas locais em suas tabelas de rota. Para obter mais informações, consulte [Roteamento para ClassicLink \(p. 1110\)](#).
- As VPCs configuradas para locação de hardware dedicada não podem ser habilitadas para ClassicLink. Entre em contato com o Amazon Web Services Support para solicitar que a VPC da sua locação dedicada possa ser habilitada para ClassicLink.

Important

As instâncias do EC2-Classic são executadas em hardware compartilhado. Se você definiu a locação da sua VPC como dedicated por conta de requisitos regulamentares ou de segurança, vincular uma instância do EC2-Classic à sua VPC pode não estar em conformidade com esses requisitos, pois isso permite que um recurso de locação compartilhado aborde seus recursos isolados diretamente usando endereços IP privados. Se você precisa habilitar sua VPC dedicada para o ClassicLink, forneça um motivo detalhado na sua solicitação para o Amazon Web Services Support.

- Se você vincular sua instância do EC2-Classic a uma VPC no intervalo 172.16.0.0/16 e tiver um servidor DNS em execução no endereço IP 172.16.0.23/32 dentro da VPC, sua instância vinculada do EC2-Classic não poderá acessar o servidor DNS da VPC. Para contornar esse problema, execute seu servidor DNS em um endereço IP diferente dentro da VPC.
- O ClassicLink não oferece suporte a relacionamentos transitivos fora da VPC. Sua instância vinculada do EC2-Classic não terá acesso a nenhuma conexão VPN, endpoint de gateway de VPC, gateway NAT ou Internet Gateway associados à VPC. Da mesma forma, os recursos do outro lado de uma conexão VPN ou de um Internet Gateway não terão acesso a uma instância vinculada do EC2-Classic.

Trabalhar com ClassicLink

Você pode usar os consoles do Amazon EC2 e do Amazon VPC para trabalhar com o recurso ClassicLink. Você pode habilitar ou desabilitar uma VPC para ClassicLink e vincular e desvincular instâncias do EC2-Classic a uma VPC.

Note

Os recursos do ClassicLink só podem ser vistos nos consoles para contas e regiões que oferecem suporte a EC2-Classic.

Tarefas

- [Habilitar VPC para ClassicLink \(p. 1112\)](#)
- [Criar uma VPC com ClassicLink habilitado \(p. 1112\)](#)
- [Vincular a uma instância a uma VPC \(p. 1112\)](#)
- [Vincular uma instância a uma VPC na execução \(p. 1113\)](#)
- [Visualizar suas VPCs habilitadas para ClassicLink e as instâncias vinculadas \(p. 1113\)](#)
- [Habilitar o suporte a DNS do ClassicLink \(p. 1113\)](#)
- [Desabilitar o suporte a DNS do ClassicLink \(p. 1114\)](#)

- [Desvincular uma instância de uma VPC \(p. 1114\)](#)
- [Desabilitar ClassicLink para uma VPC \(p. 1114\)](#)

Habilitar VPC para ClassicLink

Para vincular uma instância do EC2-Classic a uma VPC, você deve primeiro habilitar a VPC para ClassicLink. Você não poderá habilitar uma VPC para ClassicLink se a VPC tiver um roteamento que entra em conflito com o intervalo de endereços IP privados do EC2-Classic. Para obter mais informações, consulte [Roteamento para ClassicLink \(p. 1110\)](#).

Para habilitar a VPC para ClassicLink

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecionar a VPC
4. Escolha Actions (Ações), Enable ClassicLink (Habilitar ClassicLink).
5. Quando a confirmação for solicitada, escolha Enable ClassicLink (Habilitar ClassicLink).
6. (Opcional) Se você quiser que o hostname de DNS público resolva para o endereço IP privado, habilite o suporte a DNS do ClassicLink para a VPC antes de vincular qualquer instância. Para obter mais informações, consulte [Habilitar o suporte a DNS do ClassicLink \(p. 1113\)](#).

Criar uma VPC com ClassicLink habilitado

Você pode criar uma nova VPC e imediatamente habilitá-la para o ClassicLink usando o assistente da VPC no console da Amazon VPC.

Para criar uma VPC com ClassicLink habilitado

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel da Amazon VPC, selecione Launch VPC Wizard (Iniciar assistente da VPC).
3. Selecione uma das opções de configuração de VPC e escolha Select (Selecionar).
4. Na página seguinte do assistente, escolha Yes (Sim) para Enable ClassicLink (Habilitar o ClassicLink). Conclua o restante das etapas do assistente para criar sua VPC. Para obter mais informações sobre como usar o assistente de VPC, consulte [Cenários da Amazon VPC](#) no Guia do usuário da Amazon VPC.
5. (Opcional) Se você quiser que o hostname de DNS público resolva para o endereço IP privado, habilite o suporte a DNS do ClassicLink para a VPC antes de vincular qualquer instância. Para obter mais informações, consulte [Habilitar o suporte a DNS do ClassicLink \(p. 1113\)](#).

Vincular a uma instância a uma VPC

Depois de habilitar uma VPC para ClassicLink, você pode vincular uma instância do EC2-Classic a ela. A instância deve estar no estado `running`.

Se você quiser que o hostname de DNS público resolva para o endereço IP privado, habilite o suporte a DNS do ClassicLink para a VPC antes de vincular a instância. Para obter mais informações, consulte [Habilitar o suporte a DNS do ClassicLink \(p. 1113\)](#).

Para vincular a uma instância a uma VPC

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).

3. Selecione uma ou mais instâncias do EC2-Classic em execução.
4. Escolha Actions (Ações), ClassicLink, Link to VPC (Vincular à VPC).
5. Escolha a VPC. O console exibe apenas VPCs habilitadas para ClassicLink.
6. Selecione um ou mais dos grupos de segurança para associar às instâncias. O console exibe grupos de segurança apenas de VPCs habilitadas para ClassicLink.
7. Escolha Link.

Vincular uma instância a uma VPC na execução

Você pode usar o assistente de lançamento no console do Amazon EC2 para executar uma instância do EC2-Classic e imediatamente vinculá-la a uma VPC habilitada para ClassicLink.

Para vincular uma instância a uma VPC na execução

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel do Amazon EC2, escolha Launch Instance (Executar instância).
3. Selecione uma AMI e depois escolha um tipo de instância compatível com o EC2-Classic. Para obter mais informações, consulte [Tipos de instância disponíveis no EC2-Classic \(p. 1101\)](#).
4. Na página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:
 - a. Em Network (Rede), escolha Launch into EC2-Classic (Executar no EC2-Classic). Se essa opção estiver desabilitada, o tipo de instância não será compatível com o EC2-Classic.
 - b. Expanda Link to VPC (ClassicLink) (Vincular à VPC (ClassicLink)) e escolha uma VPC em Link to VPC (Vincular à VPC). O console exibe apenas VPCs com o ClassicLink habilitado.
5. Conclua as demais etapas do assistente para executar a instância. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).

Visualizar suas VPCs habilitadas para ClassicLink e as instâncias vinculadas

Você pode visualizar todas as VPCs habilitadas para ClassicLink no console do Amazon VPC e suas instâncias do EC2-Classic vinculadas no console do Amazon EC2.

Para ver suas VPCs habilitadas por ClassicLink

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecionar a VPC
4. Se o valor de ClassicLink for Enabled (Habilitado), a VPC está habilitada para ClassicLink.

Habilitar o suporte a DNS do ClassicLink

Você pode habilitar o suporte a DNS do ClassicLink para sua VPC de forma que os hostnames de DNS sejam endereçados entre instâncias vinculadas do EC2-Classic e instâncias na resolução da VPC para endereços IP privados e não para endereços IP públicos. Para esse recurso funcionar, sua VPC deve ser habilitada para hostnames de DNS e resolução de DNS.

Note

Se você habilitar suporte a DNS do ClassicLink para sua VPC, sua instância do EC2-Classic vinculada pode acessar qualquer zona hospedada privada associada à VPC. Para obter mais informações, consulte [Como trabalhar com zonas hospedadas privadas](#) no Guia do desenvolvedor do Amazon Route 53.

Para habilitar o suporte a DNS do ClassicLink

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecionar a VPC
4. Escolha Actions (Ações), Edit ClassicLink DNS Support (Editar suporte de DNS do ClassicLink).
5. Para ClassicLink DNS support (Suporte de DNS do ClassicLink), selecione Enable (Habilitar).
6. Selecione Save changes (Salvar alterações).

Desabilitar o suporte a DNS do ClassicLink

Você pode desabilitar o suporte a DNS do ClassicLink para sua VPC de forma que os hostnames de DNS sejam endereçados entre instâncias vinculadas do EC2-Classic e instâncias na resolução da VPC para endereços IP públicos e não para endereços IP privados.

Para desabilitar o suporte a DNS do ClassicLink

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecionar a VPC
4. Escolha Actions (Ações), Edit ClassicLink DNS Support (Editar suporte de DNS do ClassicLink).
5. Para ClassicLink DNS Support (Suporte de DNS do ClassicLink), desmarque Enable (Habilitar).
6. Selecione Save changes (Salvar alterações).

Desvincular uma instância de uma VPC

Se você não precisar mais da conexão com o ClassicLink entre a instância do EC2-Classic e sua VPC, pode desvincular a instância da VPC. Desvincular a instância dissocia os security groups de VPC da instância.

Uma instância interrompida é automaticamente desvinculada de uma VPC.

Para desvincular uma instância da VPC

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma ou mais de suas instâncias.
4. Escolha Actions (Ações), ClassicLink, Unlink from VPC (Desvincular da VPC).
5. Quando a confirmação for solicitada, escolha Unlink (Desvincular).

Desabilitar ClassicLink para uma VPC

Se você não precisar mais de uma conexão entre as instâncias do EC2-Classic e sua VPC, pode desativar o ClassicLink na VPC. Primeiro desvincule todas as instâncias vinculadas do EC2-Classic que sejam vinculadas à VPC.

Para desabilitar ClassicLink para uma VPC

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione a VPC.

4. Escolha Actions (Ações), Disable ClassicLink (Desabilitar ClassicLink).
5. Quando a confirmação for solicitada, escolha Disable ClassicLink (Desabilitar ClassicLink).

Exemplos de políticas do IAM para ClassicLink

Você pode habilitar uma VPC para o ClassicLink e, em seguida, vincular a instância do EC2-Classic à VPC. Você também pode visualizar as VPC habilitadas para o ClassicLink e todas as instâncias do EC2-Classic que estão vinculadas a uma VPC. Você pode criar políticas com permissão em nível de recurso para as ações `ec2:EnableVpcClassicLink`, `ec2:DisableVpcClassicLink`, `ec2:AttachClassicLinkVpc` e `ec2:DetachClassicLinkVpc` para controlar como os usuários podem usar essas ações. As permissões em nível de recurso não são compatíveis com ações `ec2:Describe*`.

Exemplos

- [Permissões completas para trabalhar com o ClassicLink \(p. 1115\)](#)
- [Habilitar e desabilitar uma VPC para o ClassicLink \(p. 1115\)](#)
- [Vincular instâncias \(p. 1116\)](#)
- [Desvincular instâncias \(p. 1116\)](#)

Permissões completas para trabalhar com o ClassicLink

A política a seguir concede aos usuários permissões para exibir VPCs habilitadas para o ClassicLink e instâncias do EC2-Classic vinculadas, habilitar e desabilitar uma VPC para o ClassicLink, e vincular e desvincular instâncias em uma VPC habilitada para o ClassicLink.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeClassicLinkInstances", "ec2:DescribeVpcClassicLink",  
                "ec2:EnableVpcClassicLink", "ec2:DisableVpcClassicLink",  
                "ec2:AttachClassicLinkVpc", "ec2:DetachClassicLinkVpc"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Habilitar e desabilitar uma VPC para o ClassicLink

A política a seguir permite que o usuário habilite ou desabilite VPCs para o ClassicLink que tenham a tag "específica 'purpose=classiclink'. Os usuários não podem habilitar ou desabilitar nenhuma outra VPC para o ClassicLink.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:*VpcClassicLink",  
            "Resource": "arn:aws:ec2:region:account:vpc/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/purpose": "classiclink"  
                }  
            }  
        }  
    ]  
}
```

```
        }
    ]
}
```

Vincular instâncias

A política a seguir concede aos usuários permissões para vincular instâncias a uma VPC somente se a instância for um tipo de instância m3.large. A segunda declaração permite que os usuários usem a VPC e os recursos do security group que são necessários para vincular uma instância a uma VPC.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:AttachClassicLinkVpc",
      "Resource": "arn:aws:ec2:region:account:instance/*",
      "Condition": {
        "StringEquals": {
          "ec2:InstanceType": "m3.large"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:AttachClassicLinkVpc",
      "Resource": [
        "arn:aws:ec2:region:account:vpc/*",
        "arn:aws:ec2:region:account:security-group/*"
      ]
    }
  ]
}
```

A política a seguir concede aos usuários permissões para vincular instâncias somente a uma VPC específica (vpc-1a2b3c4d) e associar somente security groups específicos da VPC à instância (sg-1122aabb e sg-aabb2233). Os usuários não podem vincular uma instância a nenhuma outra VPC e não podem especificar nenhum outro security group da VPC para associação com a instância na solicitação.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:AttachClassicLinkVpc",
      "Resource": [
        "arn:aws:ec2:region:account:vpc/vpc-1a2b3c4d",
        "arn:aws:ec2:region:account:instance/*",
        "arn:aws:ec2:region:account:security-group/sg-1122aabb",
        "arn:aws:ec2:region:account:security-group/sg-aabb2233"
      ]
    }
  ]
}
```

Desvincular instâncias

O seguinte concede permissão aos usuários para desvincular qualquer instância do EC2-Classic vinculada de uma VPC, mas somente se a instância tiver a tag "unlink=true". A segunda instrução concede aos

usuários permissões para usar o recurso da VPC, que é necessário para desvincular uma instância de uma VPC.

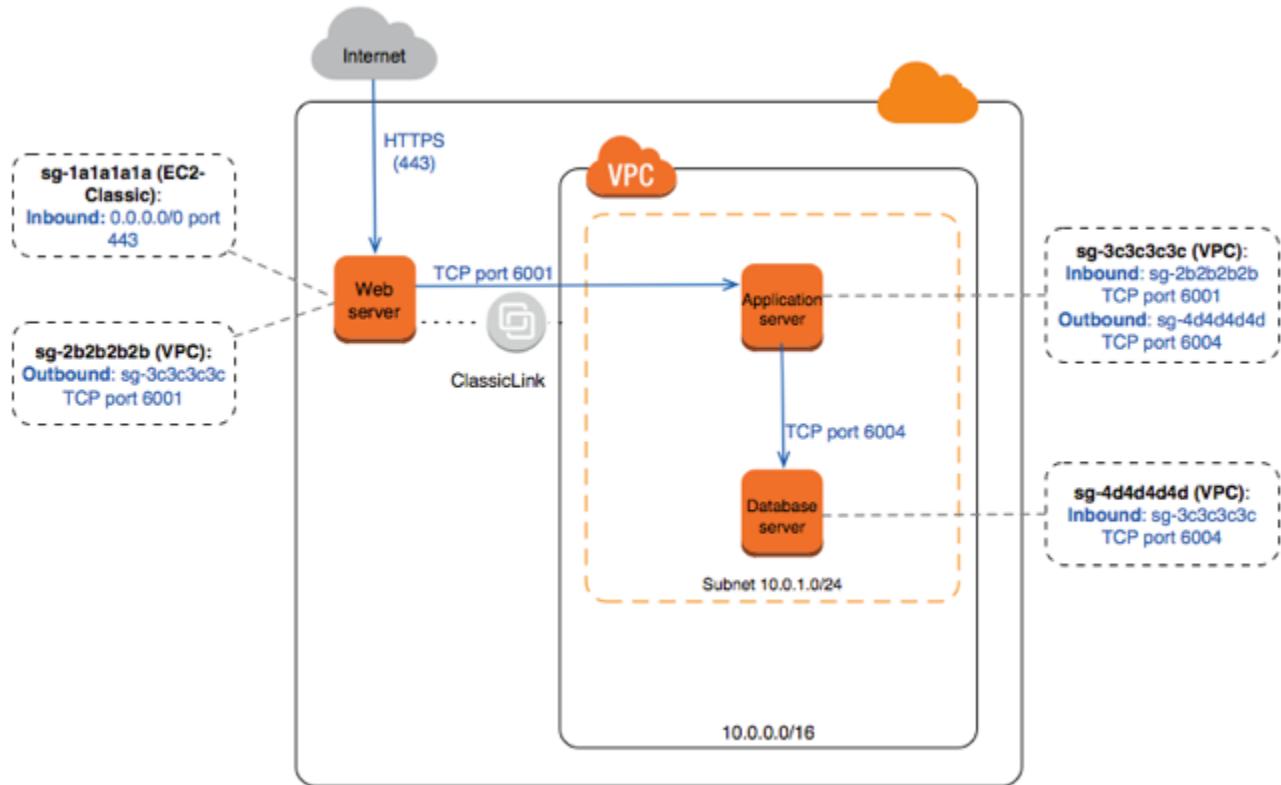
```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": "ec2:DetachClassicLinkVpc",  
        "Resource": [  
            "arn:aws:ec2:region:account:instance/*"  
        ],  
        "Condition": {  
            "StringEquals": {  
                "ec2:ResourceTag/unlink": "true"  
            }  
        }  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2:DetachClassicLinkVpc",  
        "Resource": [  
            "arn:aws:ec2:region:account:vpc/*"  
        ]  
    }  
}
```

Exemplo: configuração do grupo de segurança do ClassicLink para uma aplicação Web de três níveis

Neste exemplo, você tem uma aplicação com três instâncias: um servidor Web voltado ao público, um servidor de aplicações e um servidor de banco de dados. Seu servidor Web aceita o tráfego HTTPS da Internet e se comunica com seu servidor de aplicações pela porta TCP 6001. Seu servidor de aplicações então se comunica com seu servidor de banco de dados pela porta TCP 6004. Você está no processo de migrar sua aplicação inteira para uma VPC na sua conta. Você já migrou seu servidor de aplicações e seu servidor de banco de dados para a VPC. Seu servidor Web ainda está no EC2-Classic e vinculado à sua VPC via ClassicLink.

Você quer uma configuração do security group que permita que o tráfego flua somente entre essas instâncias. Você tem quatro security groups: dois para seu servidor Web (sg-1a1a1a1a e sg-2b2b2b2b), um para seu servidor de aplicações (sg-3c3c3c3c) e um para seu servidor de banco de dados (sg-4d4d4d4d).

O diagrama a seguir exibe a arquitetura das suas instâncias e a configuração do seu security group.



Grupos de segurança do servidor Web (**sg-1a1a1a1a** e **sg-2b2b2b2b**)

Vocês têm um security group no EC2-Classic e o outro na sua VPC. Você associou o security group da VPC à instância do servidor Web ao ligar a instância à sua VPC via ClassicLink. O security group da VPC permite que você controle o tráfego de saída do seu servidor Web para o servidor de aplicações.

A seguir estão as regras para grupos de segurança da EC2-Classic (**sg-1a1a1a1a**).

Inbound			
Origem	Tipo	Intervalo de portas	Comentários
0.0.0.0/0	HTTPS	443	Permite que o tráfego da Internet alcance seu servidor Web.

A seguir estão as regras do security group para o security group da VPC (**sg-2b2b2b2b**).

Outbound			
Destino	Tipo	Intervalo de portas	Comentários
sg-3c3c3c3c	TCP	6001	Permite tráfego de saída do seu servidor Web para seu servidor de aplicações na sua VPC (ou a alguma outra)

instância associada com
sg-3c3c3c3c).

Grupo de segurança para servidor de aplicações (**sg-3c3c3c3c**)

A seguir estão as regras do security group para o security group da VPC associada com seu servidor de aplicações.

Inbound			
Origem	Tipo	Intervalo de portas	Comentários
sg-2b2b2b2b	TCP	6001	Permite o tipo de tráfego especificado do seu servidor Web (ou qualquer outra instância associada com sg-2b2b2b2b) alcance seu servidor de aplicações.
Outbound			
Destino	Tipo	Intervalo de portas	Comentários
sg-4d4d4d4d	TCP	6004	Allows outbound traffic from the application server to the database server (or to any other instance associated with sg-4d4d4d4d).

Grupo de segurança para servidor de banco de dados (**sg-4d4d4d4d**)

A seguir estão as regras do security group para o security group da VPC associada com seu servidor de banco de dados.

Inbound			
Origem	Tipo	Intervalo de portas	Comentários
sg-3c3c3c3c	TCP	6004	Permite o tipo de tráfego especificado do seu servidor de aplicações (ou qualquer outra instância associada com sg-3c3c3c3c) alcance seu servidor de banco de dados.

Migre do EC2-Classic para uma VPC

Caso tenha criado sua conta da AWS antes de 4 de dezembro de 2013, talvez você tenha suporte para o EC2-Classic em algumas regiões da AWS. Alguns recursos e funções do Amazon EC2, como

redes aprimoradas e tipos de instância mais novos, precisam de uma virtual private cloud (VPC). Alguns recursos podem ser compartilhados entre EC2-Classic e uma VPC, e alguns não podem. Para obter mais informações, consulte [Compartilhar e acessar recursos entre EC2-Classic e uma VPC \(p. 1106\)](#). É recomendável migrar para uma VPC para aproveitar os recursos de somente VPC.

Para migrar do EC2-Classic para uma VPC, você deve migrar ou recriar seus recursos do EC2-Classic em uma VPC. Você pode migrar e recriar seus recursos completamente ou executar uma migração incremental ao longo do tempo usando o ClassicLink.

Tópicos

- [Opções para obter uma VPC padrão \(p. 1120\)](#)
- [Migrar seus recursos para uma VPC \(p. 1121\)](#)
- [Usar ClassicLink para uma migração incremental \(p. 1125\)](#)
- [Exemplo: Migrar uma aplicação Web simples \(p. 1126\)](#)

Opções para obter uma VPC padrão

Uma VPC padrão é uma VPC configurada e pronta para usar e está disponível somente em regiões que são somente VPC. Para regiões compatíveis com o EC2-Classic, você pode criar uma VPC não padrão para configurar seus recursos. No entanto, talvez você queira usar uma VPC padrão se preferir não configurar você mesmo uma VPC ou se não tiver requisitos específicos para a configuração da VPC. Para obter mais informações sobre as VPCs padrão, consulte [VPC padrão e sub-redes padrão](#) no Guia do usuário da Amazon VPC.

Veja a seguir as opções para usar uma VPC padrão quando você tem uma conta da AWS compatível com o EC2-Classic.

Opções

- [Mudar para uma região somente VPC \(p. 1120\)](#)
- [Criar uma nova conta da AWS \(p. 1120\)](#)
- [Converter a conta da AWS existente em somente VPC \(p. 1120\)](#)

Mudar para uma região somente VPC

Use essa opção se quiser usar sua conta existente para configurar seus recursos em uma VPC padrão e não precisar usar uma região específica. Para localizar uma região que tenha uma VPC padrão, consulte [Detectar plataformas suportadas \(p. 1099\)](#).

Criar uma nova conta da AWS

As novas contas da AWS são compatíveis somente com VPC. Use essa opção se desejar uma conta que tenha uma VPC padrão em todas as regiões.

Converter a conta da AWS existente em somente VPC

Use essa opção se desejar uma VPC padrão em todas as regiões da sua conta existente. Para poder converter sua conta, você deve excluir todos os recursos do EC2-Classic. Você também pode migrar alguns recursos para uma VPC. Para obter mais informações, consulte [Migrar seus recursos para uma VPC \(p. 1121\)](#).

Como converter sua conta do EC2-Classic

1. Exclua ou migre (se aplicável) os recursos que você criou para uso no EC2-Classic. Incluindo o seguinte:

- Instâncias do Amazon EC2
 - Os grupos de segurança do EC2-Classic (excluindo o grupo de segurança padrão, que você não pode excluir)
 - Endereços IP elásticos do EC2-Classic
 - Classic Load Balancers
 - Recursos do Amazon RDS
 - Recursos do Amazon ElastiCache
 - Recursos do Amazon Redshift
 - AWS Elastic BeanstalkRecursos do
 - AWS Data PipelineRecursos do
 - Recursos do Amazon EMR
 - AWS OpsWorksRecursos do
2. Acesse a Central de suporte da Amazon Web Services em console.aws.amazon.com/support.
 3. Selecione Create case (Criar caso).
 4. Escolha Suporte à conta e ao faturamento.
 5. Em Tipo, escolha Conta. Em Categoria, escolha Converter EC2 Classic em VPC.
 6. Preencha os outros detalhes conforme necessário e escolha Enviar. Analisaremos sua solicitação e entraremos em contato com você para orientá-lo pelas próximas etapas.

Migrar seus recursos para uma VPC

Você pode migrar ou mover alguns de seus recursos para uma VPC. Alguns recursos só podem ser migrados do EC2-Classic para uma VPC que esteja na mesma região e na mesma conta da AWS. Se o recurso não puder ser migrado, você deverá criar um novo recurso para uso na VPC.

Prerequisites

Antes de começar, você deve ter uma VPC. Se você não tiver uma VPC padrão, poderá criar uma VPC não padrão usando um destes métodos:

- No console da Amazon VPC, use o assistente de VPC para criar uma nova VPC. Para obter mais informações, consulte [Configurações do Assistente do Console da Amazon VPC](#). Use essa opção se quiser configurar uma VPC rapidamente usando uma das opções de configuração disponíveis.
- No console da Amazon VPC, configure os componentes de uma VPC de acordo com seus requisitos. Para obter mais informações, consulte [VPCs e sub-redes](#). Use essa opção se houver requisitos específicos para sua VPC, como um número específico de sub-redes.

Tópicos

- [Grupos de segurança \(p. 1121\)](#)
- [Endereços IP elásticos \(p. 1122\)](#)
- [AMIs e instâncias \(p. 1122\)](#)
- [Instâncias de banco de dados do Amazon RDS \(p. 1125\)](#)

Grupos de segurança

No entanto, se você quiser que as instâncias de sua VPC tenham as mesmas regras de grupo de segurança das instâncias do EC2-Classic, você poderá usar o console do Amazon EC2 para copiar as regras do grupo de segurança existentes do EC2-Classic para um novo grupo de segurança da VPC.

Somente é possível copiar as regras do grupo de segurança para um novo grupo de segurança na conta da AWS na mesma região. Se você estiver usando uma região ou conta da AWS diferente, crie um novo grupo de segurança e adicione as regras manualmente. Para obter mais informações, consulte [Grupos de segurança do Amazon EC2 para instâncias do Windows \(p. 1217\)](#).

Para copiar as regras do security group para um novo security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança associado à instância do EC2-Classic, escolha Ações e selecione Copiar para novo.

Note

Para identificar um grupo de segurança do EC2-Classic, verifique a coluna ID da VPC. Para cada grupo de segurança do EC2-Classic, o valor na coluna está em branco ou tem um símbolo –.

4. Na caixa de diálogo Create Security Group, especifique um nome e uma descrição para o novo security group. Selecione a VPC na lista VPC.
5. A guia Inbound (Entrada) é preenchida com as regras do grupo de segurança do seu EC2-Classic. Você pode modificar as regras conforme o necessário. Na guia Outbound, uma regra que permite todo tráfego de saída foi criada automaticamente para você. Para obter mais informações sobre como modificar regras do security group, consulte [Grupos de segurança do Amazon EC2 para instâncias do Windows \(p. 1217\)](#).

Note

Se tiver definido uma regra no grupo de segurança do EC2-Classic que faz referência a outro grupo de segurança, você não poderá usar a mesma regra em um grupo de segurança da VPC. Modifique a regra para fazer referência a um security group na mesma VPC.

6. Escolha Create (Criar).

Endereços IP elásticos

Você pode migrar um endereço IP elástico alocado para uso no EC2-Classic para uso com uma VPC. Não é possível migrar um endereço IP elástico para outra região ou conta da AWS. Para obter mais informações, consulte [Migrar um endereço IP elástico do EC2-Classic \(p. 1104\)](#).

Para identificar um endereço IP elástico alocado para uso no EC2-Classic

No console do Amazon EC2, escolha IPs elásticos no painel de navegação. Na coluna Escopo o valor é padrão.

Como alternativa, use o seguinte comando `describe-addresses`.

```
aws ec2 describe-addresses --filters Name=domain,Values=standard
```

AMIs e instâncias

Uma AMI é um modelo para executar a instância do Amazon EC2. Você pode criar sua própria AMI com base em uma instância do EC2-Classic existente e usar essa AMI para executar instâncias em sua VPC.

Tópicos

- [Identificar instâncias do EC2-Classic \(p. 1123\)](#)
- [Criar uma AMI \(p. 1123\)](#)
- [\(Opcional\) Compartilhar ou copiar a AMI \(p. 1124\)](#)

- [\(Opcional\) Armazenar os dados em volumes do Amazon EBS \(p. 1124\)](#)
- [Executar uma instância na VPC \(p. 1124\)](#)

Identificar instâncias do EC2-Classic

Se você tiver instâncias em execução no EC2-Classic e em uma VPC, poderá identificar suas instâncias do EC2-Classic.

Console do Amazon EC2

No painel de navegação, escolha Instances (Instâncias). Na coluna ID da VPC, o valor para cada instância do EC2-Classic está em branco ou tem um símbolo -. Se a coluna VPC ID (ID da VPC) não estiver presente, escolha o ícone de engrenagem e torne a coluna visível.

AWS CLI

Use o seguinte comando [describe-instances](#) da AWS CLI. O parâmetro --query exibe apenas as instâncias nas quais o valor de VpcId é null.

```
aws ec2 describe-instances --query 'Reservations[*].Instances[?VpcId==`null`]'
```

Criar uma AMI

Depois de identificar a instância do EC2-Classic, você pode criar uma AMI a partir dela.

Como criar uma AMI do Windows

Para obter mais informações, consulte [Criar uma AMI do Windows personalizada](#).

Como criar uma AMI do Linux

O método usado para criar a AMI do Linux depende do tipo de dispositivo raiz da instância e da plataforma do sistema operacional na qual a instância é executada. Para descobrir qual é o tipo de dispositivo raiz de sua instância, acesse a página Instances, selecione sua instância e veja as informações no campo Root device type na guia Description. Se o valor for ebs, sua instância é baseada em EBS. Se o valor for instance-store, sua instância é com armazenamento de instâncias. Você também pode usar o comando da AWS CLI [describe-instances](#) para descobrir o tipo de dispositivo raiz.

A tabela a seguir fornece opções para você criar a AMI do Linux de acordo com o tipo de dispositivo raiz de sua instância e da plataforma de software.

Important

Alguns tipos de instâncias oferecem suporte aos tipos de virtualização de HVM e de PV, enquanto outras oferecem suporte a apenas um ou outro. Se você planeja usar sua AMI para executar um tipo de instância diferente do tipo de instância atual, verifique se o tipo de instância é compatível com o tipo de virtualização que a AMI oferece. Se a AMI for compatível com a virtualização PV e você quiser usar um tipo de instância que seja compatível com a virtualização de HVM, talvez seja necessário reinstalar o software em uma AMI de HVM de base. Para obter mais informações sobre virtualização PV e de HVM, consulte [Tipos de virtualização de AMI do Linux](#).

Tipo de dispositivo raiz da instância	Ação
EBS	Crie uma AMI baseada em EBS da instância. Para obter mais informações, consulte Criar uma AMI do Linux baseada no Amazon EBS .

Tipo de dispositivo raiz da instância	Ação
Armazenamento de instâncias	Crie uma AMI com armazenamento de instâncias a partir da sua instância usando as ferramentas da AMI. Para obter mais informações, consulte Criar uma AMI do Linux com armazenamento de instâncias .
Armazenamento de instâncias	Converta sua instância com armazenamento de instâncias em uma instância baseada em EBS. Para obter mais informações, consulte Converter a AMI com armazenamento de instâncias em uma AMI baseada no Amazon EBS .

(Opcional) Compartilhar ou copiar a AMI

Para usar a AMI para executar uma instância em uma nova conta da AWS, você deve primeiro compartilhar a AMI com a nova conta. Para obter mais informações, consulte [Compartilhar uma AMI com contas específicas da AWS \(p. 112\)](#).

Para usar a AMI para executar uma instância em uma VPC em uma região diferente, você deve primeiro copiar a AMI nessa região. Para obter mais informações, consulte [Copiar um AMI \(p. 120\)](#).

(Opcional) Armazenar os dados em volumes do Amazon EBS

Você pode criar um volume do Amazon EBS e usá-lo para fazer backup e armazenar os dados em sua instância—como você usaria um disco rígido físico. Os volumes do Amazon EBS podem ser anexados e desconectados de qualquer instância na mesma zona de disponibilidade. Você pode desanexar um volume de sua instância no EC2-Classic e anexá-lo a uma nova instância que você executa na VPC na mesma zona de disponibilidade.

Para obter mais informações sobre volumes de Amazon EBS consulte os seguintes tópicos:

- [Volumes do Amazon EBS \(p. 1245\)](#)
- [Crie um volume do Amazon EBS. \(p. 1268\)](#)
- [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#)

Para fazer backup dos dados no volume de Amazon EBS, você pode gerar snapshots periódicos do volume. Para obter mais informações, consulte [Criar snapshots de Amazon EBS \(p. 1298\)](#). Se você precisar, poderá restaurar um volume do Amazon EBS de seu snapshot. Para obter mais informações, consulte [Criar um volume a partir de um snapshot \(p. 1270\)](#).

Executar uma instância na VPC

Depois de criar uma AMI, você pode usar o assistente de inicialização do Amazon EC2 para executar uma instância na VPC. A instância terá os mesmos dados e configurações da instância do EC2-Classic existente.

Note

Você pode usar essa oportunidade para [fazer upgrade para um tipo de instância de geração atual](#).

Para executar uma instância na VPC

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel, escolha Executar instância.
3. Na página Choose an Amazon Machine Image, selecione a categoria My AMIs e selecione a AMI que você criou. Como alternativa, se você compartilhou uma AMI de outra conta, na lista de filtro de

Propriedade escolha Compartilhada comigo. Selecione a AMI que você compartilhou em sua conta do EC2-Classic.

4. Na página Choose an Instance Type, selecione o tipo de instância e escolha Next: Configure Instance Details.
5. Na página Configure Instance Details, selecione sua VPC na lista Network. Selecione a sub-rede necessária na lista Subnet. Configure todos os outros detalhes necessários e passe para as próximas páginas do assistente até chegar à página Configurar grupo de segurança.
6. Selecione Selecionar um grupo existente e escolha o grupo de segurança que você criou para a VPC. Escolha Review and Launch.
7. Reveja os detalhes da instância e selecione Launch para especificar um par de chaves e executar a instância.

Para obter mais informações sobre os parâmetros que você pode configurar em cada etapa do assistente, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#).

Instâncias de banco de dados do Amazon RDS

Você pode mover sua instância de banco de dados do EC2-Classic para uma VPC na mesma região, na mesma conta. Para obter mais informações, consulte [Atualizar a VPC para uma instância de banco de dados](#) no Guia do usuário da Amazon RDS.

Usar ClassicLink para uma migração incremental

O recurso ClassicLink facilita o gerenciamento de uma migração incremental para uma VPC. O ClassicLink permite vincular uma instância do EC2-Classic a uma VPC em sua conta na mesma região, permitindo que os novos recursos da VPC se comuniquem com a instância do EC2-Classic usando endereços IPv4 privados. Depois, você pode migrar a funcionalidade de um componente de cada vez até que a aplicação esteja sendo executada totalmente na VPC.

Use essa opção se você não puder permitir tempo de inatividade durante a migração, por exemplo, se você tiver uma aplicação de várias camadas com processos que não podem ser interrompidos.

Para obter mais informações sobre ClassicLink, consulte [ClassicLink \(p. 1107\)](#).

Tarefas

- [Etapa 1: Preparar a sequência de migração \(p. 1125\)](#)
- [Etapa 2: Habilitar a VPC para o ClassicLink \(p. 1126\)](#)
- [Etapa 3: Vincular as instâncias do EC2-Classic à VPC \(p. 1126\)](#)
- [Etapa 4: Concluir a migração da VPC \(p. 1126\)](#)

Etapa 1: Preparar a sequência de migração

Para usar o ClassicLink com eficácia, primeiro você deve identificar os componentes de sua aplicação que devem ser migrados para a VPC e confirmar a ordem na qual essa funcionalidade será migrada.

Por exemplo, você tem uma aplicação que conta com um servidor Web de apresentação, um servidor de banco de dados de backend e a lógica de autenticação para transações. Você pode decidir iniciar o processo de migração com a lógica de autenticação, depois com o servidor de banco de dados e, finalmente, com o servidor Web.

Depois, você pode começar a migrar ou a recriar seus recursos. Para obter mais informações, consulte [Migrar seus recursos para uma VPC \(p. 1121\)](#).

Etapa 2: Habilitar a VPC para o ClassicLink

Após configurar as novas instâncias da VPC e tornar a funcionalidade da aplicação disponível na VPC, você poderá usar o ClassicLink para permitir a comunicação de IP privado entre as novas instâncias da VPC e as instâncias do EC2-Classic. Primeiro, você deve habilitar a VPC para o ClassicLink.

Para habilitar a VPC para ClassicLink

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Your VPCs (Suas VPCs).
3. Selecione uma VPC.
4. Escolha Actions (Ações), Enable ClassicLink (Habilitar ClassicLink).
5. Quando a confirmação for solicitada, escolha Enable ClassicLink (Habilitar ClassicLink).

Etapa 3: Vincular as instâncias do EC2-Classic à VPC

Depois de habilitar o ClassicLink na VPC, você pode vincular as instâncias do EC2-Classic à VPC. A instância deve estar no estado `running`.

Para vincular a uma instância a uma VPC

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma ou mais instâncias do EC2-Classic em execução.
4. Escolha Actions (Ações), ClassicLink, Link to VPC (Vincular à VPC).
5. Escolha uma VPC. O console exibe apenas VPCs habilitadas para ClassicLink.
6. Selecione um ou mais dos grupos de segurança para associar às instâncias. O console exibe grupos de segurança apenas de VPCs habilitadas para ClassicLink.
7. Escolha Link.

Etapa 4: Concluir a migração da VPC

Dependendo do tamanho da aplicação e da funcionalidade que deve ser migrada, repita as etapas anteriores até transferir todos os componentes da aplicação do EC2-Classic para a VPC.

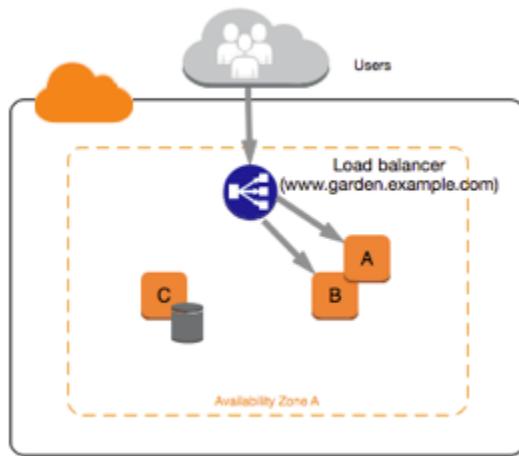
Após habilitar a comunicação interna entre o EC2-Classic e as instâncias de VPC, você deverá atualizar sua aplicação para apontar para o serviço migrado em sua VPC, em vez do serviço na plataforma do EC2-Classic. As etapas exatas dependem do design de sua aplicação. Geralmente, isso inclui a atualização de seus endereços IP de destino para apontar para os endereços IP de suas instâncias de VPC, e não para as instâncias do EC2-Classic.

Após concluir esta etapa e testar se a aplicação está funcionando de sua VPC, você poderá encerrar as instâncias do EC2-Classic e desativar o ClassicLink para sua VPC. Você também pode limpar todos os recursos do EC2-Classic dos quais não precisa mais para evitar cobranças deles. Por exemplo, você pode liberar endereços IP elásticos e excluir os volumes que foram associados às instâncias do EC2-Classic.

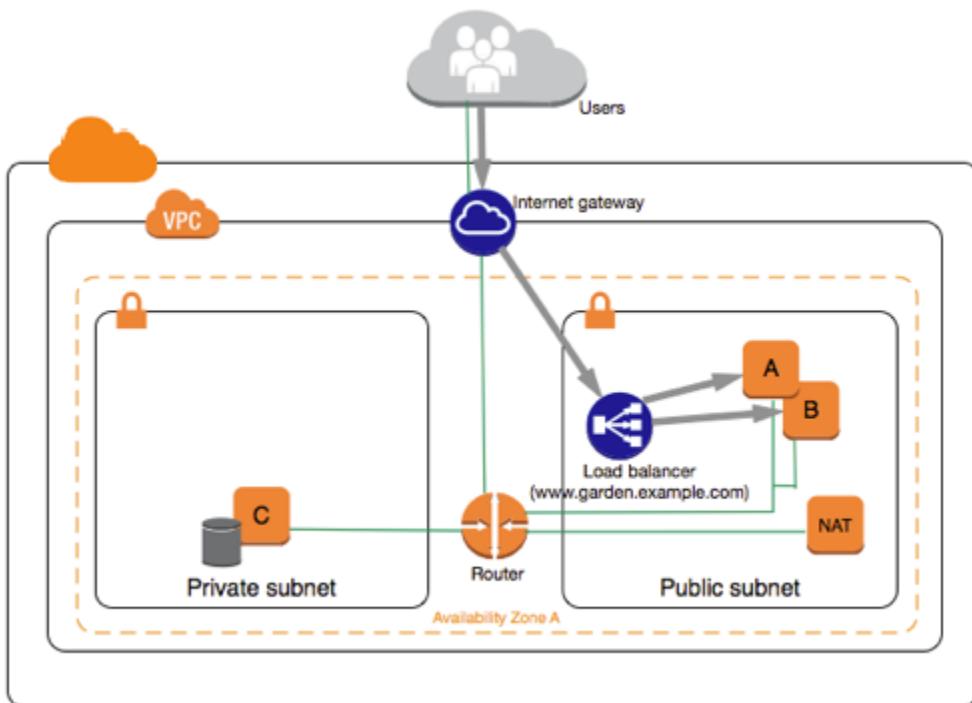
Exemplo: Migrar uma aplicação Web simples

Neste exemplo, você usa a AWS para hospedar seu site de jardinagem. Para gerenciar seu site, você tem três instâncias em execução no EC2-Classic. As instâncias A e B hospedam sua aplicação Web voltada para o público, e você usa o Elastic Load Balancing para balancear a carga do tráfego entre essas instâncias. Você atribuiu endereços IP elásticos às instâncias A e B, de modo que há endereços IP estáticos para tarefas de configuração e administração nessas instâncias. A instância C contém o banco

de dados MySQL do site. Você registrou o nome de domínio `www.garden.example.com` e usou o Route 53 para criar uma zona hospedada com um conjunto de registros de alias que está associado ao nome DNS do平衡ador de carga.



A primeira parte da migração para uma VPC é decidir o tipo de arquitetura da VPC adequado para suas necessidades. Nesse caso, você decidiu o seguinte: uma sub-rede pública para seus servidores Web e uma sub-rede privada para seu servidor de banco de dados. À medida que seu site cresce, você pode adicionar mais servidores Web e servidores de banco de dados a suas sub-redes. Por padrão, as instâncias na sub-rede privada não podem acessar a Internet. Contudo, você pode permitir acesso à Internet por meio de um dispositivo de conversão de endereços de rede (NAT) na sub-rede pública. Talvez você queira configurar um dispositivo NAT para oferecer suporte a atualizações periódicas e patches na Internet para seu servidor de banco de dados. Você migrará os endereços IP elásticos para uma VPC e criará um load balancer em sua sub-rede pública para balancear a carga do tráfego entre os servidores Web.



Para migrar sua aplicação Web para uma VPC, você pode seguir essas etapas:

- Criar uma VPC: nesse caso, você pode usar o assistente da VPC no console da Amazon VPC para criar sua VPC e sub-redes. A segunda configuração do assistente cria uma VPC com uma sub-rede privada e uma pública, e executa e configura um dispositivo de NAT em sua sub-rede pública para você. Para obter mais informações, consulte [VPC com sub-redes privadas e públicas \(NAT\)](#) no Guia do usuário da Amazon VPC.
- Configurar seus grupos de segurança: no ambiente do EC2-Classic, você tem um grupo de segurança para seus servidores Web e outro grupo de segurança para seu servidor de banco de dados. Você pode usar o console do Amazon EC2 para copiar as regras de cada security group em novos security groups para sua VPC. Para obter mais informações, consulte [Grupos de segurança \(p. 1121\)](#).

Tip

Crie os security groups que são referenciados por outros security groups primeiro.

- Criar AMIs e executar novas instâncias: crie uma AMI em um dos servidores Web e uma segunda AMI no servidor de banco de dados. Depois, execute servidores Web de substituição na sub-rede pública e execute o servidor de banco de dados de substituição na sub-rede privada. Para obter mais informações, consulte [Criar uma AMI \(p. 1123\)](#).
- Configurar o dispositivo NAT: se estiver usando uma instância NAT, você deverá criar um grupo de segurança para ela que permita o tráfego HTTP e HTTPS da sub-rede privada. Para obter mais informações, consulte [Instâncias NAT](#). Se você estiver usando um gateway de NAT, o tráfego de sua sub-rede privada será permitido automaticamente.
- Configurar o banco de dados: quando você criou uma AMI do servidor de banco de dados no EC2-Classic, todas as informações de configuração que foram armazenadas nessa instância foram copiadas na AMI. Talvez seja necessário conectar-se ao novo servidor de banco de dados e atualizar os detalhes da configuração. Por exemplo, se você configurou o banco de dados para conceder permissões completas de leitura, gravação e modificação aos servidores Web no EC2-Classic, será necessário atualizar os arquivos de configuração para conceder as mesmas permissões aos novos servidores Web da VPC.
- Configurar seus servidores Web: os servidores Web terão as mesmas definições de configuração de suas instâncias no EC2-Classic. Por exemplo, se você tiver configurado seus servidores Web para usar o banco de dados no EC2-Classic, atualize as definições de configuração de seus servidores Web para apontar para sua nova instância de banco de dados.

Note

Por padrão, as instâncias executadas em uma sub-rede não padrão recebem um endereço IP público, a menos que haja especificação em contrário durante a execução. O novo servidor de banco de dados pode não ter um endereço IP público. Nesse caso, você pode atualizar o arquivo de configuração de seus servidores Web para usar o novo nome DNS privado do servidor de banco de dados. As instâncias na mesma VPC podem se comunicar pelo endereço IP privado.

- Migrar os endereços IP elásticos: desassocie os endereços IP elásticos de seus servidores Web no EC2-Classic e migre-os em seguida para uma VPC. Após migrá-los, você pode associá-los a seus novos servidores Web em sua VPC. Para obter mais informações, consulte [Migrar um endereço IP elástico do EC2-Classic \(p. 1104\)](#).
- Criar um novo load balancer: para continuar usando o Elastic Load Balancing para balancear a carga do tráfego de suas instâncias, você deve compreender as diferentes maneiras de configurar seu load balancer na VPC. Para obter mais informações, consulte o [Manual do usuário do Elastic Load Balancing](#).
- Atualizar seus registros DNS: após configurar o load balancer na sub-rede pública, verifique se o domínio `www.garden.example.com` aponta para o novo load balancer. Para fazer isso, atualize os registros DNS e o registro de alias definido no Route 53. Para obter mais informações sobre como usar o Route 53, consulte [Introdução ao Route 53](#).
- Desligar os recursos do EC2-Classic: após verificar se sua aplicação Web está trabalhando de dentro de arquitetura de VPC, você pode desligar os recursos do EC2-Classic para parar de receber cobranças referentes a eles.

Segurança no Amazon EC2

A segurança da nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se beneficiará de um datacenter e de uma arquitetura de rede criados para atender aos requisitos das empresas com as maiores exigências de segurança.

A segurança é uma responsabilidade compartilhada entre a AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos [Programas de conformidade da AWS](#). Para saber mais sobre os programas de compatibilidade que se aplicam ao Amazon EC2, consulte [Serviços da AWS em escopo por programa de compatibilidade](#).
- Segurança na nuvem: sua responsabilidade inclui as seguintes áreas:
 - Controlar o acesso à rede para as instâncias, por exemplo, por meio da configuração da VPC e dos grupos de segurança. Para obter mais informações, consulte [Controlar o tráfego de rede \(p. 1130\)](#).
 - Gerenciar as credenciais usadas para a conexão às instâncias.
 - Gerenciar o sistema operacional convidado e o software implantado no sistema operacional convidado, incluindo atualizações e patches de segurança. Para obter mais informações, consulte [Gerenciamento de atualizações no Amazon EC2 \(p. 1239\)](#).
 - Configurar as funções do IAM anexadas à instância e as permissões associadas a estas funções. Para obter mais informações, consulte [Funções do IAM para Amazon EC2 \(p. 1195\)](#).

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon EC2. Ela mostra como configurar o Amazon EC2 para atender aos objetivos de segurança e conformidade. Saiba também como usar outros serviços da AWS que ajudam você a monitorar e proteger os recursos do Amazon EC2.

Para obter as melhores práticas de segurança para o Amazon EC2 executar o Windows Server, consulte Segurança e rede em [Melhores práticas do Windows no Amazon EC2 \(p. 19\)](#).

Tópicos

- [Segurança da infraestrutura no Amazon EC2 \(p. 1130\)](#)
- [Amazon EC2 e VPC endpoints de interface \(p. 1132\)](#)
- [Resiliência no Amazon EC2 \(p. 1133\)](#)
- [Proteção de dados no Amazon EC2 \(p. 1134\)](#)
- [Identity and Access Management para o Amazon EC2 \(p. 1137\)](#)
- [Pares de chaves do Amazon EC2 e instâncias do Windows \(p. 1209\)](#)
- [Grupos de segurança do Amazon EC2 para instâncias do Windows \(p. 1217\)](#)
- [Gerenciamento de configuração no Amazon EC2 \(p. 1238\)](#)
- [Gerenciamento de atualizações no Amazon EC2 \(p. 1239\)](#)
- [Gerenciamento de alterações no Amazon EC2 \(p. 1239\)](#)
- [Validação de conformidade do Amazon EC2 \(p. 1239\)](#)
- [Auditoria e responsabilidade no Amazon EC2 \(p. 1240\)](#)

Segurança da infraestrutura no Amazon EC2

Como um serviço gerenciado, o Amazon EC2 é protegido pelos procedimentos de segurança de rede global da AWS que estão descritos no whitepaper [Amazon Web Services: visão geral dos processos de segurança](#).

Você usa chamadas à API publicadas pela AWS para acessar o Amazon EC2 por meio da rede. Os clientes devem oferecer suporte a Transport Layer Security (TLS) 1.0 ou posterior. Recomendamos TLS 1.2 ou posterior. Os clientes também devem ter suporte a conjuntos de criptografia com perfect forward secrecy (PFS) como Ephemeral Diffie-Hellman (DHE) ou Ephemeral Elliptic Curve Diffie-Hellman (ECDHE). A maioria dos sistemas modernos como Java 7 e versões posteriores oferece suporte a esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Isolamento de rede

Uma nuvem virtual privada (VPC) é uma rede virtual na área isolada logicamente na Nuvem AWS. Use VPCs separadas para isolar a infraestrutura por workload ou entidade organizacional.

Uma sub-rede é um intervalo de endereços IP em uma VPC. Quando executa uma instância, você a executa em uma sub-rede em sua VPC. Use sub-redes para isolar as camadas de sua aplicação (por exemplo, Web, aplicação e banco de dados) em uma única VPC. Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet.

Para chamar a API do Amazon EC2 em sua VPC sem enviar tráfego pela Internet pública, use o AWS PrivateLink.

Isolamento em hosts físicos

Diferentes instâncias do EC2 no mesmo host físico são isoladasumas das outras como se estivessem em hosts físicos separados. O hipervisor isola a CPU e a memória, e as instâncias recebem discos virtualizados em vez de acesso aos dispositivos de disco bruto.

Quando você interrompe ou encerra uma instância, a memória alocada para ela é apagada (definida como zero) pelo hipervisor antes que ela seja alocada para uma nova instância, e cada bloco de armazenamento é redefinido. Isso garante que seus dados não sejam expostos acidentalmente para outra instância.

Os endereços MAC de rede são atribuídos dinamicamente às instâncias pela infraestrutura da rede da AWS. Os endereços IP são atribuídos dinamicamente a instâncias pela infraestrutura de rede da AWS ou atribuídos por um administrador do EC2 por meio de solicitações autenticadas da API. A rede da AWS permite que as instâncias enviem tráfego somente de endereços MAC e IP atribuídos a elas. Caso contrário, o tráfego será descartado.

Por padrão, uma instância não pode receber tráfego que não seja endereçado especificamente a ela. Se for necessário executar a conversão de endereço de rede (NAT), o roteamento ou os serviços de firewall em sua instância, você poderá desabilitar a verificação de origem/destino da interface de rede.

Controlar o tráfego de rede

Considere as seguintes opções de controle de tráfego de rede para suas instâncias do EC2:

- Restrinja o acesso a suas instâncias usando [grupos de segurança \(p. 1217\)](#). Configure os grupos de segurança da instância do Amazon EC2 a fim de permitir o tráfego de rede mínimo necessário para a

instância do Amazon EC2 e permitir o acesso somente de locais definidos, esperados e aprovados. Por exemplo, se uma instância do Amazon EC2 for um servidor Web IIS, configure os grupos de segurança para permitir somente HTTP/HTTPS de entrada, tráfego de gerenciamento do Windows e conexões mínimas de saída.

- Use os grupos de segurança como o mecanismo primário a fim de controlar o acesso à rede para instâncias do Amazon EC2. Quando necessário, use as ACLs de rede para fornecer controle de rede sem estado e de alta granularidade. Os grupos de segurança são mais versáteis que as ACLs de rede devido à capacidade de realizar a filtragem de pacotes com estado e criar regras que fazem referência a outros grupos de segurança. No entanto, as ACLs de rede podem ser eficientes como um controle secundário para negar um subconjunto ou tráfego específico ou fornecer grades de proteção de sub-rede de alto nível. Além disso, como as ACLs de rede se aplicam a toda uma sub-rede, elas podem ser usadas como defesa em profundidade caso uma instância seja iniciada de forma não intencional sem um grupo de segurança correto.
- Gerencie centralmente as configurações do Firewall do Windows com os Objetos de Política de Grupo (GPO) para aprimorar ainda mais os controles de rede. Os clientes costumam usar o Firewall do Windows para obter maior visibilidade do tráfego de rede e para complementar os filtros de grupo de segurança, criando regras avançadas para impedir que aplicações específicas acessem a rede ou filtrem o tráfego de endereços IP de um subconjunto. Por exemplo, o Firewall do Windows pode limitar o acesso ao endereço IP do serviço de metadados do EC2 para usuários ou aplicações específicas. Como alternativa, um serviço voltado para o público pode usar grupos de segurança para restringir o tráfego a portas específicas e o Firewall do Windows a manter uma lista negra de endereços IP explicitamente bloqueados.
- Ao gerenciar instâncias do Windows, limite o acesso a alguns servidores de gerenciamento centralizados bem definidos ou bastion hosts para reduzir a superfície de ataque do ambiente. Além disso, use protocolos de administração seguros, como encapsulamento de RDP sobre SSL/TLS. O Quick Start para Gateway de Desktop Remoto fornece as melhores práticas para implantar um gateway de desktop remoto remota, incluindo a configuração de RDP para usar SSL/TLS.
- Use o Active Directory ou AWS Directory Service para controlar central e rigorosamente e monitorar o acesso de usuário interativo e grupo às instâncias do Windows, além de evitar permissões de usuário local. Evite também usar Administradores de domínio e, em vez disso, crie contas baseadas em função mais granulares e específicas para a aplicação. A Administração Suficiente (JEA) permite que as alterações nas instâncias do Windows sejam gerenciadas sem acesso interativo ou de administrador. Além disso, a JEA permite que as organizações bloqueiem o acesso administrativo ao subconjunto dos comandos do Windows PowerShell necessários para a administração da instância. Para obter informações adicionais, consulte a seção "Gerenciar o acesso ao Amazon EC2 no nível do sistema operacional" no whitepaper [AWS Security Best Practices](#) (Práticas recomendadas de segurança da AWS).
- Os administradores de sistema devem usar as contas do Windows com acesso limitado para realizar atividades diárias e somente elevar o acesso quando necessário para realizar alterações de configuração específicas. Além disso, somente acesse as instâncias do Windows diretamente quando absolutamente necessário. Em vez disso, use os sistemas de gerenciamento de configuração central, como o Run Command do EC2, o Systems Center Configuration Manager (SCCM), o Windows PowerShell DSC ou o Amazon EC2 Systems Manager (SSM), para enviar as alterações aos servidores Windows.
- Configure as tabelas de rotas de sub-rede da Amazon VPC com as rotas de rede mínimas necessárias. Por exemplo, insira somente as instâncias do Amazon EC2 que exigem acesso direto à Internet nas sub-redes com rotas para um gateway da Internet e insira somente instâncias do Amazon EC2 que precisem de acesso direto a redes internas nas sub-redes com rotas para um gateway privado virtual.
- Considere usar grupos de segurança adicionais ou ENIs para controlar e auditar o tráfego de gerenciamento de instâncias do Amazon EC2 separadamente do tráfego de aplicações regular. Esta abordagem permite que os clientes implementem políticas do IAM especiais para o controle de alterações, facilitando a auditoria de alterações às regras de grupo de segurança ou scripts automáticos de verificação de regras. Várias ENIs também fornecem opções adicionais para controlar o tráfego de rede, incluindo a capacidade de criar políticas de roteamento baseado em host ou usar diferentes regras de roteamento de sub-rede da VPC com base na sub-rede atribuída da ENI.

- Use o AWS Virtual Private Network ou o AWS Direct Connect para estabelecer conexões privadas de suas redes remotas com suas VPCs. Para obter mais informações, consulte [Opções de conectividade entre a rede e a Amazon VPC](#).
- Use [Logs de fluxo da VPC](#) para monitorar o tráfego recebido nas instâncias.
- Use o [AWS Security Hub](#) para verificar acessibilidade de rede acidental nas instâncias.
- Use o [Gerenciador de sessões do AWS Systems Manager](#) para acessar suas instâncias remotamente em vez de abrir Portas RDP.
- Use o [Run Command do AWS Systems Manager](#) para automatizar tarefas administrativas em vez de abrir Portas RDP.
- Muitas das funções do SO Windows e das aplicações de negócios da Microsoft também oferecem funcionalidade aprimorada, como restrições de intervalo de endereços IP no IIS, políticas de filtragem TCP/IP no Microsoft SQL Server e políticas de filtro de conexão no Microsoft Exchange. A funcionalidade de restrição de rede na camada de aplicação pode fornecer camadas adicionais de defesa para servidores de aplicação de negócios críticos.

Além de restringir o acesso à rede para cada instância do Amazon EC2, a Amazon VPC oferece suporte à implementação de controles de segurança de rede adicionais, como gateways em linha, servidores de proxy e várias opções de monitoramento de rede.

Para obter mais informações, consulte o whitepaper [AWS Security Best Practices](#) (Práticas recomendadas de segurança da AWS).

Amazon EC2 e VPC endpoints de interface

É possível melhorar a postura de segurança da sua VPC configurando o Amazon EC2 para usar um VPC endpoint de interface. Os endpoints de interface são ativados por AWS PrivateLink , uma tecnologia que permite acessar APIs do Amazon EC2 de forma privada restringindo todo o tráfego de rede entre sua VPC e o Amazon EC2 à rede da Amazon. Com endpoints de interface, também não são necessários um gateway da Internet, um dispositivo NAT nem um gateway privado virtual.

Não é necessário configurar o AWS PrivateLink , mas é recomendável. Para obter mais informações sobre o AWS PrivateLink e os VPC endpoints, consulte [VPC endpoints de interface \(AWS PrivateLink\)](#).

Tópicos

- [Criar um VPC endpoint de interface \(p. 1132\)](#)
- [Criar uma política de VPC endpoint de interface \(p. 1132\)](#)

Criar um VPC endpoint de interface

Crie um endpoint para o Amazon EC2 usando o seguinte nome de serviço:

- **com.amazonaws.*region*.ec2** — cria um endpoint para as ações da API do Amazon EC2.

Para obter mais informações, consulte [Criar um endpoint de interface](#) no Guia do usuário da Amazon VPC.

Criar uma política de VPC endpoint de interface

É possível associar uma política ao seu VPC endpoint para controlar o acesso à API do Amazon EC2. A política especifica:

- O principal que pode executar ações.

- As ações que podem ser executadas.
- O recurso no qual as ações podem ser executadas.

Important

Quando uma política não padrão é aplicada a um endpoint da VPC de interface para o Amazon EC2, determinadas solicitações de API com falha, como as com falha de RequestLimitExceeded, podem não ser registradas no AWS CloudTrail nem no Amazon CloudWatch.

Para obter mais informações, consulte [Controlar o acesso a serviços com VPC endpoints](#) no Guia do usuário da Amazon VPC.

O exemplo a seguir mostra uma política de VPC endpoint que nega permissão para criar volumes não criptografados ou executar instâncias com volumes não criptografados. O exemplo de política também concede permissão para executar todas as outras ações do Amazon EC2.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Action": "ec2:*",  
            "Effect": "Allow",  
            "Resource": "*",  
            "Principal": "*"  
        },  
        {  
            "Action": [  
                "ec2:CreateVolume"  
            ],  
            "Effect": "Deny",  
            "Resource": "*",  
            "Principal": "*",  
            "Condition": {  
                "Bool": {  
                    "ec2:Encrypted": "false"  
                }  
            }  
        },  
        {  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Effect": "Deny",  
            "Resource": "*",  
            "Principal": "*",  
            "Condition": {  
                "Bool": {  
                    "ec2:Encrypted": "false"  
                }  
            }  
        }  
    ]  
}
```

Resiliência no Amazon EC2

A infraestrutura global da AWS é criada com base em regiões e zonas de disponibilidade da AWS. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas

com baixa latência, altas taxas de transferência e redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Se você precisar replicar seus dados ou aplicações para distâncias geográficas maiores, use as Local Zones da AWS. Uma Local Zone da AWS é uma extensão de uma região da AWS na proximidade geográfica de seus usuários. As Local Zones têm suas próprias conexões com a Internet e suporte no AWS Direct Connect. Como todas as regiões da AWS, as Local Zones da AWS são completamente isoladas de outras zonas da AWS.

Se você precisar replicar seus dados ou aplicações em uma Local Zone da AWS, a AWS recomenda que você use uma das seguintes zonas como zona de failover:

- Outra Local Zone
- Uma zona de disponibilidade na região que não é a zona principal. Você pode usar o comando [describe-availability-zones](#) para visualizar a zona principal.

Para obter mais informações sobre regiões e zonas de disponibilidade da AWS, consulte [Infraestrutura global da AWS](#).

Além da infraestrutura global da AWS, o Amazon EC2 oferece os seguintes recursos para oferecer suporte à resiliência de seus dados:

- Copiar AMIs entre regiões
- Copiar snapshots do EBS entre regiões
- Automatizando AMIs suportadas por EBS usando o Amazon Data Lifecycle Manager
- Automatizar snapshots do EBS usando o Amazon Data Lifecycle Manager
- Manter a integridade e a disponibilidade da frota usando o Amazon EC2 Auto Scaling
- Distribuir o tráfego de entrada entre instâncias em uma única zona de disponibilidade ou em várias zonas de disponibilidade usando o Elastic Load Balancing.

Proteção de dados no Amazon EC2

O [modelo de responsabilidade compartilhada](#) da AWS se aplica à proteção de dados no Amazon Elastic Compute Cloud. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança dos serviços da AWS que você usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas frequentes sobre privacidade de dados](#). Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and GDPR](#) no Blog de segurança da AWS.

Para fins de proteção de dados, recomendamos que você proteja as credenciais da conta da Conta da AWS e configure as contas de usuário individuais com o AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Recomendamos TLS 1.2 ou posterior.
- Configure o registro em log das atividades da API e do usuário com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão nos serviços da AWS.

- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para obter mais informações sobre endpoints do FIPS, consulte [Federal Information Processing Standard \(FIPS\) 140-2](#).

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso também vale para o uso do Amazon EC2 ou de outros produtos da AWS com o console, a API, a AWS CLI ou os AWS SDKs. Quaisquer dados inseridos em marcações ou campos de formato livre usados para nomes podem ser usados para logs de cobrança ou diagnóstico. Se fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Criptografia em repouso

Volumes do EBS

A criptografia do Amazon EBS é uma solução de criptografia para snapshots e volumes do EBS. Ele usa a AWS KMS keys. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).

Você também pode usar permissões do Microsoft EFS e NTFS para criptografia em nível de pasta e arquivo.

Volumes de armazenamento de instâncias

Os dados nos volumes de armazenamento de instâncias de NVMe são criptografados usando uma criptografia XTS-AES-256 implementada em um módulo de hardware na instância. As chaves de criptografia são geradas usando o módulo de hardware e são exclusivas para cada dispositivo de armazenamento de instâncias de NVMe. Todas as chaves de criptografia são destruídas quando a instância é interrompida ou encerrada e não podem ser recuperadas. Você não pode desativar essa criptografia e não pode fornecer sua própria chave de criptografia.

Os dados em volumes de armazenamento de instância HDD em instâncias H1, D3 e D3en são criptografados usando XTS-AES-256 e chaves de uso único.

Memory

A criptografia de memória está habilitada nas seguintes instâncias:

- Instâncias com processadores AWS Graviton 2, como instâncias M6g. Esses processadores são compatíveis com criptografia de memória sempre ativa. As chaves de criptografia são geradas com segurança dentro do sistema host, não saem do sistema host e são destruídas quando o host é reinicializado ou desligado.
- Instâncias com processadores Intel Xeon escalável (Ice Lake), como instâncias M6i. Esses processadores são compatíveis com criptografia de memória sempre ativa usando a Intel Total Memory Encryption (TME).

Criptografia em trânsito

Criptografia na camada física

Todos os dados fluindo pelas regiões da AWS por meio da rede global da AWS é automaticamente criptografada na camada física antes de sair das instalações seguras da AWS. Todo o tráfego entre AZs é

criptografado. Camadas adicionais de criptografia, inclusive as listadas nesta seção, podem fornecer mais proteções.

Criptografia fornecida pelo emparelhamento da Amazon VPC e do Transit Gateway entre regiões

Todo o tráfego entre regiões que usa o emparelhamento da Amazon VPC e do Transit Gateway é automaticamente criptografado em massa ao sair de uma região. Uma camada adicional de criptografia é fornecida automaticamente à camada física para todo o tráfego entre regiões, conforme observado anteriormente nesta seção.

Criptografia entre instâncias

AWSA fornece conectividade privada e segura entre instâncias do EC2 de todos os tipos. Além disso, alguns tipos de instância usam os recursos de descarregamento do hardware subjacente Nitro System para criptografar automaticamente o tráfego em trânsito entre instâncias, usando algoritmos AEAD com criptografia de 256 bits. Não há impacto na performance da rede. Para oferecer suporte a essa criptografia adicional de tráfego em trânsito entre instâncias, os seguintes requisitos devem ser atendidos:

- As instâncias utilizam os seguintes tipos de instância:
 - Uso geral: M5dn | M5n | M5zn | M6i
 - Otimizada para computação: C5a | C5ad | C5n
 - Memória otimizada: R5dn | R5n | alta memória (u-*), apenas virtualizada
 - Otimizada para armazenamento: D3 | D3en | I3en
 - Computação acelerada: G4ad | G4dn | P3dn
- As instâncias estão na mesma região.
- As instâncias estão na mesma VPC ou VPCs emparelhadas, e o tráfego não passa por um dispositivo ou serviço de rede virtual, como um平衡ador de carga ou um gateway de trânsito.

Uma camada adicional de criptografia é fornecida automaticamente à camada física para todo o tráfego antes que ele saia das instalações seguras da AWS, conforme observado anteriormente nesta seção.

Para exibir os tipos de instância que criptografam o tráfego em trânsito entre instâncias usando o AWS CLI

Use o comando [describe-instance-types](#) a seguir.

```
aws ec2 describe-instance-types \
--filters Name=network-info.encryption-in-transit-supported,Values=true \
--query "InstanceTypes[*].[InstanceType]" --output text
```

Criptografia de e para o AWS Outposts

Um Outpost cria conexões de rede especiais chamadas links de serviço à região da AWS inicial e, opcionalmente, conectividade privada com uma sub-rede da VPC especificada. Todo o tráfego que passa por essas conexões é totalmente criptografado. Para obter mais informações, consulte [Conectividade por meio de links de serviço](#) e [Criptografia em trânsito](#) no Manual do usuário do AWS Outposts.

Criptografia de acesso remoto

O RDP fornece um canal de comunicação seguro para o acesso remoto às instâncias do Windows, seja diretamente, seja por meio do EC2 Instance Connect. O acesso remoto às instâncias que usam Session Manager do AWS Systems Manager e o Run Command é criptografado usando TLS 1.2, e as solicitações para criar uma conexão são assinadas usando [SigV4](#) e são autenticadas e autorizadas pelo [AWS Identity and Access Management](#).

É de sua responsabilidade usar um protocolo de criptografia, como o Transport Layer Security (TLS), para criptografar dados sigilosos em trânsito entre clientes e suas instâncias do Amazon EC2.

Permita somente conexões criptografadas entre instâncias do EC2 e os endpoints de API da AWS ou outros serviços de rede remota confidenciais. Isso pode ser imposto por meio do uso de grupo de segurança de saída ou regras de [Firewall do Windows](#).

Identity and Access Management para o Amazon EC2

As credenciais de segurança identificam você para os serviços na AWS e concedem uso ilimitado dos recursos da AWS, como os recursos do Amazon EC2. Você pode usar recursos do Amazon EC2 e do AWS Identity and Access Management (IAM) para permitir que outros usuários, serviços e aplicações usem seus recursos do Amazon EC2 sem compartilhar suas credenciais de segurança. Você pode usar o IAM para controlar como outros usuários usam recursos em sua conta da AWS, e usar os grupos de segurança para controlar o acesso às instâncias do Amazon EC2. Você pode escolher permitir uso completo ou limitado dos recursos do Amazon EC2.

Tópicos

- [Acesso à rede para a instância \(p. 1137\)](#)
- [Atributos de permissões do Amazon EC2 \(p. 1137\)](#)
- [IAM e Amazon EC2 \(p. 1138\)](#)
- [Políticas do IAM no Amazon EC2 \(p. 1139\)](#)
- [Políticas gerenciadas da AWS para o Amazon Elastic Compute Cloud \(p. 1194\)](#)
- [Funções do IAM para Amazon EC2 \(p. 1195\)](#)
- [Autorizar tráfego de entrada para suas instâncias do Windows \(p. 1205\)](#)

Acesso à rede para a instância

Um security group atua como um firewall que controla o tráfego permitido para acessar uma ou mais instâncias. Quando executa uma instância, você atribui um ou mais security groups a ela. Para cada security group, você adiciona regras que controlam o tráfego para a instância. Você pode modificar as regras de um security group a qualquer momento. As novas regras são aplicadas automaticamente a todas as instâncias associadas ao security group.

Para obter mais informações, consulte [Autorizar tráfego de entrada para suas instâncias do Windows \(p. 1205\)](#).

Atributos de permissões do Amazon EC2

Sua organização pode ter várias contas da AWS. O Amazon EC2 permite que você especifique contas adicionais da AWS que podem usar as Imagens de máquinas da Amazon (AMIs) e snapshots do Amazon EBS. Essas permissões funcionam somente em nível de conta da AWS. Você não pode restringir as permissões a usuários específicos na conta da AWS especificada. Todos os usuários na conta da AWS que você especifica podem usar a AMI ou o snapshot.

Cada AMI tem um atributo `LaunchPermission` que controla quais contas da AWS podem acessar a AMI. Para obter mais informações, consulte [Tornar um AMI pública \(p. 110\)](#).

Cada snapshot do Amazon EBS tem um atributo `createVolumePermission` que controla quais contas da AWS podem usar o snapshot. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#).

IAM e Amazon EC2

O IAM permite que você:

- Criar usuários e grupos na conta da AWS
- Atribua credenciais de segurança exclusivas a cada usuário em sua conta da AWS
- Controle as permissões de cada usuário para executar tarefas usando recursos da AWS
- Permita que os usuários em outra conta da AWS compartilhem seus recursos da AWS
- Crie funções para sua conta da AWS e defina os usuários ou os serviços que podem assumi-las
- Use identidades existentes em sua empresa a fim de conceder permissões para executar tarefas usando recursos da AWS

Ao usar o IAM com o Amazon EC2, você pode controlar se os usuários de sua organização podem executar uma tarefa usando ações específicas da API do Amazon EC2 e se podem usar recursos específicos da AWS.

Este tópico ajuda a responder as seguintes questões:

- Como criar grupos e usuários no IAM?
- Como criar uma política?
- Quais políticas do IAM são necessárias para realizar tarefas no Amazon EC2?
- Como conceder permissões para executar ações no Amazon EC2?
- Como conceder permissões para executar ações em recursos específicos do Amazon EC2?

Criar um grupo e usuários do IAM

Para criar um grupo do IAM

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Groups e escolha, Create New Group.
3. Em Group Name (Nome do grupo), insira um nome para o grupo e selecione Next Step (Próxima etapa).
4. Na página Attach Policy, selecione uma política gerenciada da AWS e escolha Next Step. Por exemplo, para o Amazon EC2, uma das seguintes políticas gerenciadas pela AWS pode atender às suas necessidades:
 - PowerUserAccess
 - ReadOnlyAccess
 - AmazonEC2FullAccess
 - AmazonEC2ReadOnlyAccess
5. Escolha Create Group.

O grupo novo é listado em Group Name (Nome do grupo).

Para criar um usuário do IAM, adicionar o usuário ao grupo e criar uma senha para o usuário

1. No painel de navegação, escolha Users, Add user.
2. Em User name (Nome de usuário), insira um nome de usuário.
3. Em Access type, selecione Programmatic access e AWS Management Consoleaccess.

4. Em Console password, selecione uma das opções a seguir:
 - Autogenerated password. Cada usuário obtém uma senha gerada de forma aleatória que atenda à política de senha atual em vigor (se houver). Você pode visualizar ou fazer download das senhas ao acessar a página Final.
 - Custom password. A cada usuário é atribuída a senha inserida na caixa.
5. Escolha Próximo: Permissões.
6. Na página Definir permissões, escolha Adicionar usuário ao grupo. Marque a caixa de seleção ao lado do grupo que você criou anteriormente e escolha Próximo: Revisar.
7. Escolha Criar usuário.
8. Para visualizar as chaves de acesso dos usuários (IDs de chave de acesso e chaves de acesso secretas), escolha Show ao lado de cada senha e chave de acesso secreta que você deseja ver. Para salvar as chaves de acesso, escolha Fazer download de .csv e, em seguida, salve o arquivo em um local seguro.

Important

Não é possível recuperar a chave de acesso secreta depois de concluir essa etapa. Se você a perder, deverá criar uma nova.

9. Escolha Close (Fechar).
10. Forneça as credenciais (chaves de acesso e senha) a cada usuário. Isso permite que os usuários usem os serviços com base nas permissões que você especificou para o grupo do IAM.

Tópicos relacionados

Para obter mais informações sobre IAM, consulte o seguinte:

- [Políticas do IAM no Amazon EC2 \(p. 1139\)](#)
- [Funções do IAM para Amazon EC2 \(p. 1195\)](#)
- [AWS Identity and Access Management \(IAM\)](#)
- [Manual do usuário do IAM](#)

Políticas do IAM no Amazon EC2

Por padrão, os usuários do IAM não têm permissão para criar ou modificar recursos do Amazon EC2 ou para executar tarefas usando a API do Amazon EC2. (Isso significa que eles também não podem fazer isso usando o console do Amazon EC2 ou a CLI.) Para permitir que os usuários do IAM criem ou modifiquem recursos e realizem tarefas, você deve criar políticas do IAM que concedam aos usuários do IAM permissão para usar os recursos específicos e as ações de API de que precisam e, então, anexar essas políticas aos usuários ou grupos do IAM que exijam essas permissões.

Quando você anexa uma política a um usuário ou grupo de usuários, isso concede ou nega aos usuários permissão para realizar as tarefas especificadas nos recursos especificados. Para obter mais informações gerais sobre as políticas do IAM, consulte [Permissões e políticas](#) no Guia do usuário do IAM. Para obter mais informações sobre como gerenciar e criar políticas personalizadas do IAM, consulte [Gerenciamento de políticas do IAM](#).

Conceitos básicos

Uma política do IAM deve conceder ou negar permissões para usar uma ou mais ações do Amazon EC2. Ela também deve especificar os recursos que podem ser usados com a ação, que podem ser todos os recursos ou, em alguns casos, recursos específicos. A política também pode incluir condições que você aplica ao recurso.

O Amazon EC2 oferece suporte parcial a permissões em nível de recurso. Isso significa que, para algumas operações de API do EC2, não é possível especificar com qual recurso um usuário tem permissão para trabalhar para essa ação. Em vez disso, você precisa permitir que os usuários trabalhem com todos os recursos dessa ação.

Tarefa	Tópico
Compreender a estrutura básica de uma política	Sintaxe da política (p. 1140)
Definir ações em sua política	Ações do Amazon EC2 (p. 1141)
Definir recursos específicos em sua política	Nomes de recurso da Amazon (ARNs) para o Amazon EC2 (p. 1142)
Aplicar condições ao uso dos recursos	Chaves de condição do Amazon EC2 (p. 1143)
Trabalhar com permissões disponíveis em nível de recurso para o Amazon EC2	Ações, recursos e chaves de condição para o Amazon EC2
Testar a política	Verificar se os usuários têm as permissões necessárias (p. 1144)
Gerar uma política do IAM	Gerar políticas com base na atividade de acesso
Políticas de exemplo para uma CLI ou SDK	Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK (p. 1147)
Políticas de exemplo para o console do Amazon EC2	Políticas de exemplo para trabalhar no console do Amazon EC2 (p. 1185)

Estrutura da política

Os tópicos a seguir explicam a estrutura de uma política do IAM.

Tópicos

- [Sintaxe da política \(p. 1140\)](#)
- [Ações do Amazon EC2 \(p. 1141\)](#)
- [Permissões no nível do recurso com suporte para ações de API do Amazon EC2 \(p. 1141\)](#)
- [Nomes de recurso da Amazon \(ARNs\) para o Amazon EC2 \(p. 1142\)](#)
- [Chaves de condição do Amazon EC2 \(p. 1143\)](#)
- [Verificar se os usuários têm as permissões necessárias \(p. 1144\)](#)

Sintaxe da política

A política do IAM é um documento JSON que consiste em uma ou mais declarações. Cada instrução é estruturada da maneira a seguir.

```
{  
    "Statement": [ {  
        "Effect": "effect",  
        "Action": "action",  
        "Resource": "arn",  
        "Condition": {  
            "condition": {  
                "key": "value"  
            }  
        }  
    }]
```

```
    }  
]  
}
```

Existem vários elementos que compõem uma instrução:

- Effect: o efeito pode ser `Allow` ou `Deny`. Por padrão, os usuários do IAM não têm permissão para usar recursos e ações da API. Por isso, todas as solicitações são negadas. Uma permissão explícita substitui o padrão. Uma negação explícita substitui todas as permissões.
- Action: a ação é a ação de API específica para a qual você está concedendo ou negando permissão. Para conhecer como especificar ação, consulte [Ações do Amazon EC2 \(p. 1141\)](#).
- Resource: o recurso afetado pela ação. Algumas ações de API do Amazon EC2 permitem incluir recursos específicos na política que podem ser criados ou modificados pela ação. Você especifica um recurso usando um nome de recurso da Amazon (ARN) ou usando o caractere curinga (*) para indicar que a instrução se aplica a todos os recursos. Para obter mais informações, consulte [Permissões no nível do recurso com suporte para ações de API do Amazon EC2 \(p. 1141\)](#).
- Condition: condições são opcionais. Elas podem ser usadas para controlar quando a política está em vigor. Para obter mais informações sobre como especificar condições para o Amazon EC2, consulte [Chaves de condição do Amazon EC2 \(p. 1143\)](#).

Para obter informações sobre declarações de política do IAM de exemplo para o Amazon EC2, consulte [Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK \(p. 1147\)](#).

Ações do Amazon EC2

Em uma declaração de política do IAM, você pode especificar qualquer ação de API de qualquer serviço que dê suporte ao IAM. Para o Amazon EC2, use o seguinte prefixo com o nome da ação da API: `ec2:`. Por exemplo: `ec2:RunInstances` e `ec2:CreateImage`.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, conforme o seguinte:

```
"Action": [ "ec2:action1", "ec2:action2" ]
```

Você também pode especificar várias ações usando caracteres curinga. Por exemplo, você pode especificar todas as ações cujo nome começa com a palavra "Describe" da seguinte forma:

```
"Action": "ec2:Describe*"
```

Note

No momento, as ações de API do Amazon EC2 não são compatíveis com permissões em nível de recurso. Para obter mais informações sobre permissões no nível do recurso para o Amazon EC2, consulte [Políticas do IAM no Amazon EC2 \(p. 1139\)](#).

Para especificar todas as ações de API do Amazon EC2, use o curinga `**` da seguinte maneira:

```
"Action": "ec2:***"
```

Para obter uma lista de ações de Amazon EC2, consulte [Ações definidas pelo Amazon EC2](#) na Referência de autorização do serviço.

Permissões no nível do recurso com suporte para ações de API do Amazon EC2

Permissões no nível do recurso se referem à capacidade de especificar em quais recursos os usuários têm permissão para realizar ações. O Amazon EC2 tem suporte parcial para permissões no nível do recurso.

Isso significa que, para determinadas ações do Amazon EC2, você pode controlar quando os usuários têm permissão para usar essas ações com base em condições que precisam ser concluídas, ou em recursos específicos que os usuários têm permissão para usar. Por exemplo, você pode conceder aos usuários permissões para ativar instâncias, mas apenas de um tipo específico, e usando uma AMI específica.

Para especificar um recurso em uma declaração de política do IAM, use o respectivo nome de recurso da Amazon (ARN). Para obter mais informações sobre como especificar o valor do ARN, consulte [Nomes de recurso da Amazon \(ARNs\) para o Amazon EC2 \(p. 1142\)](#). Se uma ação de API não oferecer suporte a ARNs individuais, você deverá usar um curinga (*) para especificar que todos os recursos podem ser afetados pela ação.

Para visualizar tabelas que identificam quais ações de API do Amazon EC2 oferecem suporte a permissões no nível do recurso e os ARNs e chaves de condição que você pode usar em uma política, consulte [Ações, recursos e chaves de condição do Amazon EC2](#).

Lembre-se de que você pode aplicar permissões em nível de recurso baseadas em tags às políticas do IAM que você usa para a maioria das ações da API do Amazon EC2. Isso oferece a você mais controle sobre quais recursos o usuário pode criar, modificar ou usar. Para obter mais informações, consulte [Conceder permissão para marcar recursos durante a criação \(p. 1145\)](#).

Nomes de recurso da Amazon (ARNs) para o Amazon EC2

Cada declaração de política do IAM se aplica aos recursos que você especifica usando os ARNs.

Um ARN tem a seguinte sintaxe geral:

```
arn:aws:[service]:[region]:[account]:resourceType/resourcePath
```

serviço

O serviço (por exemplo, ec2).

region

A região do recurso (por exemplo, us-east-1).

conta

O ID da conta da AWS, sem hifens (por exemplo, 123456789012).

resourceType

O tipo de recurso (por exemplo, instance).

resourcePath

Um caminho que identifica o recurso. Você pode usar o curinga * nos caminhos.

Por exemplo, é possível indicar uma instância específica (i-1234567890abcdef0) na declaração usando o ARN da maneira a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

É possível especificar todas as instâncias pertencentes a uma conta específica usando o caractere curinga * da maneira a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Também é possível especificar todos os recursos do Amazon EC2 pertencentes a uma conta específica usando o caractere curinga * da maneira a seguir.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:/*"
```

Para especificar todos os recursos ou caso uma ação de API específica não dê suporte a ARNs, use o curinga * no elemento Resource da maneira a seguir.

```
"Resource": "*"
```

Muitas ações da API do Amazon EC2 envolvem vários recursos. Por exemplo, `AttachVolume` anexa um volume do Amazon EBS a uma instância, portanto, um usuário do IAM deve ter permissões para usar o volume e a instância. Para especificar vários recursos em uma única instrução, separe seus ARNs com vírgulas, como se segue.

```
"Resource": ["arn1", "arn2"]
```

Para obter uma lista de ARNs para recursos do Amazon EC2, consulte [Tipos de recursos definidos pelo Amazon EC2](#).

Chaves de condição do Amazon EC2

Em uma instrução de política, você também pode especificar condições que controlam quando ela entrará em vigor. Cada condição contém um ou mais pares de chave-valor. As chaves de condição não diferenciam maiúsculas de minúsculas. Definimos chaves de condição em toda a AWS, além de chaves de condição específicas do serviço adicionais.

Para obter uma lista de chaves de condição específicas do serviço para o Amazon EC2, consulte [Condition keys for Amazon EC2 \(Chaves de condição para o Amazon EC2\)](#). O Amazon EC2 também implementa as chaves de condição em toda a AWS. Para obter mais informações, consulte [Informações disponíveis em todas as solicitações](#) no Guia do usuário do IAM.

Para usar uma chave de condição em sua política do IAM, use a instrução `Condition`. Por exemplo, a política a seguir concede aos usuários permissão para adicionar e remover regras de entrada e saída para qualquer grupo de segurança. Ela usa a chave de condição `ec2:Vpc` para especificar que essas ações só podem ser executadas em grupos de segurança em uma VPC específica.

```
{
"Version": "2012-10-17",
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:RevokeSecurityGroupEgress"
        ],
        "Resource": "arn:aws:ec2:region:account:security-group/*",
        "Condition": {
            "StringEquals": {
                "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
            }
        }
    }
]
```

Caso você especifique várias condições ou várias chaves em uma única condição, avaliamos essas condições usando uma operação AND lógica. Caso você especifique uma única condição com vários

valores para uma chave, avaliamos a condição usando uma operação OR lógica. Para que as permissões sejam concedidas, todas as condições devem ser atendidas.

Você também pode usar espaços reservados quando especifica as condições. Por exemplo, você pode conceder permissão a um usuário do IAM para usar recursos com um tag que especifica o seu nome do usuário do IAM. Para obter mais informações, consulte [Elementos de política do IAM: variáveis e tags](#) no Guia do usuário do IAM.

Important

Muitas chaves de condição são específicas a um recurso, e algumas ações da API usam vários recursos. Se você gravar uma política com uma chave de condição, use o elemento `Resource` da declaração para especificar o recurso ao qual a chave de condição se aplica. Caso contrário, as políticas podem impedir que os usuários executem a ação, porque a verificação da condição falha para os recursos aos quais a chave de condição não se aplica. Se você não quiser especificar um recurso, ou se escreveu o elemento `Action` da política para incluir várias ações da API, você deverá usar o tipo de condição `...IfExists` para garantir que a chave de condição seja ignorada pelos recursos que não a usam. Para obter mais informações, consulte [Condições ...IfExists](#) no Guia do usuário do IAM.

Todas as ações do Amazon EC2 oferecem suporte às chaves de condição `aws:RequestedRegion` e `ec2:Region`. Para obter mais informações, consulte [Exemplo: restringir acesso a uma região específica \(p. 1148\)](#).

A chave `ec2:SourceInstanceARN` pode ser usada para condições que especificam o ARN da instância a partir da qual é feita uma solicitação. Esta chave de condição está disponível em toda a AWS e não é específica do serviço. Para obter exemplos de políticas, consulte [Amazon EC2: anexar ou desanexar volumes em uma instância do EC2](#) e [Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS \(p. 1181\)](#). A chave `ec2:SourceInstanceARN` não pode ser usada como uma variável para preencher o ARN para o elemento `Resource` na instrução.

Para obter um exemplo de declarações de políticas para o Amazon EC2, consulte [Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK \(p. 1147\)](#).

Verificar se os usuários têm as permissões necessárias

Depois que você tiver criado uma política do IAM, recomendaremos verificar se ela concede aos usuários as permissões para usar as ações de API e os recursos específicos de que eles precisam antes de colocar a política em produção.

Primeiro, crie um usuário do IAM para fins de teste e anexe a política do IAM que você criou para o usuário de teste. Em seguida, faça uma solicitação como o usuário de teste.

Se a ação do Amazon EC2 que você está testando cria ou modifica um recurso, você deve fazer a solicitação usando o parâmetro `DryRun` (ou executar o comando da AWS CLI com a opção `--dry-run`). Nesse caso, a chamada conclui a verificação da autorização, mas não conclui a operação. Por exemplo, você pode verificar se o usuário pode encerrar uma determinada instância sem efetivamente encerrá-la. Caso o usuário de teste tenha as permissões obrigatórias, a solicitação retorna `DryRunOperation`. Do contrário, ela retorna `UnauthorizedOperation`.

Caso a política não conceda ao usuário as permissões que você esperava ou caso ela seja muito permissiva, você pode ajustar a política conforme necessário e testá-la novamente até obter os resultados desejados.

Important

Pode levar alguns minutos para que as alterações de política sejam propagadas até entrarem em vigor. Por isso, recomendamos que você aguarde cinco minutos antes de testar as atualizações da política.

Caso uma verificação de autorização falhe, a solicitação retorna uma mensagem codificada com informações de diagnóstico. Você pode decodificar a mensagem usando a ação `DecodeAuthorizationMessage`. Para obter mais informações, consulte [DecodeAuthorizationMessage](#) no AWS Security Token Service API Reference (Referência da API do AWS Security Token Service) e [decode-authorization-message](#) na AWS CLI Command Reference (Referência de comandos da AWS CLI).

Conceder permissão para marcar recursos durante a criação

Algumas ações de resource-creating da API do Amazon EC2 permitem especificar tags quando você cria o recurso. Você pode usar tags de recursos para implementar o controle baseado em atributo (ABAC). Para obter mais informações, consulte [Marcar com tag os recursos do \(p. 1555\)](#) e [Controlar o acesso aos recursos do EC2 usando tags de recursos \(p. 1147\)](#).

Para permitir que os usuários marquem recursos na criação, eles devem ter permissões para usar a ação que cria o recurso, como `ec2:RunInstances` ou `ec2:CreateVolume`. Se as tags forem especificadas na ação resource-creating, a Amazon executará autorização adicional na ação `ec2:CreateTags` para verificar se os usuários têm permissões para criar tags. Portanto, os usuários também precisam ter permissões para usar a ação `ec2:CreateTags`.

Na definição de política do IAM para a ação `ec2:CreateTags`, use o elemento `Condition` com a chave de condição `ec2:CreateAction` para conceder permissões de marcação à ação que cria o recurso.

O exemplo a seguir demonstra uma política que permite que os usuários executem instâncias e apliquem tags a instâncias e volumes durante a execução. Os usuários não têm permissão para marcar recursos existentes (não podem chamar a ação `ec2:CreateTags` diretamente).

```
{  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags"  
            ],  
            "Resource": "arn:aws:ec2:region:account:/*/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:CreateAction" : "RunInstances"  
                }  
            }  
        }  
    ]  
}
```

Da mesma forma, a política a seguir permite que os usuários criem volumes e apliquem qualquer tag aos volumes durante a criação do volume. Os usuários não têm permissão para marcar recursos existentes (não podem chamar a ação `ec2:CreateTags` diretamente).

```
{  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateVolume"  
            ]  
        }  
    ]  
}
```

```
    "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateTags"
  ],
  "Resource": "arn:aws:ec2:region:account:/*/*",
  "Condition": {
    "StringEquals": {
      "ec2:CreateAction" : "CreateVolume"
    }
  }
]
}
```

A ação `ec2:CreateTags` será avaliada somente se as tags forem aplicadas durante a ação `resource-creating`. Portanto, um usuário que tiver permissões para criar um recurso (pressupondo-se que não existam condições de marcação) não precisa de permissão para usar a ação `ec2:CreateTags` se nenhuma tag for especificada na solicitação. Contudo, se o usuário tentar criar um recurso com tags, haverá falha na solicitação se o usuário não tiver permissão para usar a ação `ec2:CreateTags`.

A ação `ec2:CreateTags` também é avaliada se as tags forem fornecidas em um modelo de execução. Para ver um exemplo de política, consulte [Tags em um modelo de execução \(p. 1169\)](#).

Controlar o acesso a tags específicas

É possível usar condições adicionais no elemento `Condition` de suas políticas do IAM para controlar as chaves de tag e os valores que podem ser aplicados aos recursos.

As chaves de condição a seguir podem ser usadas com os exemplos na seção anterior:

- `aws:RequestTag`: para indicar que uma chave de tag ou uma chave e um valor de tag específicos devem estar presentes em uma solicitação. Outras tags também podem ser especificadas na solicitação.
 - Use com o operador de condição `StringEquals` para impor uma combinação de chave e valor de tag específica, por exemplo, para impor a tag `cost-center=cc123`:

```
"StringEquals": { "aws:RequestTag/cost-center": "cc123" }
```

- Use com o operador de condição `StringLike` para impor uma chave de tag específica, por exemplo, para impor a chave de tag `purpose`:

```
"StringLike": { "aws:RequestTag/purpose": "*" }
```

- `aws:TagKeys`: para aplicar as chaves de tags usadas na solicitação.
 - Use com o modificador `ForAllValues` para impor chaves de tags específicas se forem fornecidas na solicitação (se as tags forem especificadas na solicitação, somente chaves de tags específicas são permitidas; nenhuma outra tag é permitida). Por exemplo, as chaves de tags `environment` ou `cost-center` são permitidas:

```
"ForAllValues:StringEquals": { "aws:TagKeys": [ "environment", "cost-center" ] }
```

- Use com o modificador `ForAnyValue` para impor a presença de pelo menos uma das chaves de tags especificadas na solicitação. Por exemplo, pelo menos uma das chaves de tags `environment` ou `webserver` deve estar presente na solicitação:

```
"ForAnyValue:StringEquals": { "aws:TagKeys": [ "environment", "webserver" ] }
```

Essas chaves de condição podem ser aplicadas às ações resource-creating que são compatíveis com a marcação bem como as ações `ec2:CreateTags` e `ec2:DeleteTags`. Para saber se uma ação de API do Amazon EC2 é compatível com marcação, consulte [Ações, recursos e chaves de condição para Amazon EC2](#).

Para forçar os usuários a especificarem tags quando criam um recurso, você deve usar a chave de condição `aws:RequestTag` ou a chave de condição `aws:TagKeys` com o modificador `ForAnyValue` na ação resource-creating. A ação `ec2:CreateTags` não será avaliada se um usuário não especificar tags para a ação resource-creating.

Para condições, a chave de condição não diferencia maiúsculas de minúsculas, e o valor da condição diferencia maiúsculas de minúsculas. Portanto, para aplicar a diferenciação de maiúsculas de minúsculas de uma tag, use a chave de condição `aws:TagKeys`, onde a chave da tag é especificada como um valor na condição.

Para obter exemplos de políticas do IAM, consulte [Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK \(p. 1147\)](#). Para obter mais informações sobre as condições de vários valores, consulte [Como criar uma condição que testa vários valores de chaves](#) no Guia do usuário do IAM.

Controlar o acesso aos recursos do EC2 usando tags de recursos

Ao criar uma política do IAM que conceda permissão aos usuários do IAM para usar recursos do EC2, é possível incluir informações de tag no elemento `Condition` da política para controlar o acesso com base em tags. Isso é conhecido como controle de acesso baseado em atributo (ABAC). O ABAC oferece um controle melhor sobre quais recursos um usuário pode modificar, usar ou excluir. Para obter mais informações, consulte [O que é ABAC para a AWS?](#)

Por exemplo, é possível criar uma política que permite que os usuários encerrem uma instância, mas nega a ação se a instância tiver a tag `environment=production`. Para fazer isso, use a chave de condição `ec2:ResourceTag` para permitir ou negar acesso ao recurso com base nas tags anexadas ao recurso.

```
"StringEquals": { "ec2:ResourceTag/environment": "production" }
```

Para saber se uma ação de API do Amazon EC2 oferece suporte ao controle de acesso usando a chave de condição `ec2:ResourceTag`, consulte [Ações, recursos e chaves de condição para Amazon EC2](#). Como as ações de `Describe` não oferecem suporte a permissões em nível de recurso, você deve especificá-las em uma declaração separada sem condições.

Para obter exemplos de políticas do IAM, consulte [Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK \(p. 1147\)](#).

Se você permitir ou negar aos usuários o acesso a recursos com base em tags, considere negar explicitamente aos usuários a capacidade de adicionar essas tags ou removê-las dos mesmos recursos. Caso contrário, é possível que um usuário contorne suas restrições e obtenha acesso a um recurso modificando as tags.

Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK

Os exemplos a seguir mostram declarações de políticas que você pode usar para controlar as permissões que os usuários do IAM têm para o Amazon EC2. Essas políticas são projetadas para solicitações feitas com a AWS CLI ou com o AWS SDK. Para obter exemplos de políticas para trabalhar no console do Amazon EC2, consulte [Políticas de exemplo para trabalhar no console do Amazon EC2 \(p. 1185\)](#). Para obter exemplos de políticas do IAM específicas da Amazon VPC, consulte [Identity and Access Management para a Amazon VPC](#).

Exemplos

- [Exemplo: acesso somente leitura \(p. 1148\)](#)
- [Exemplo: restringir acesso a uma região específica \(p. 1148\)](#)
- [Trabalhar com instâncias \(p. 1149\)](#)
- [Trabalhar com volumes \(p. 1151\)](#)
- [Trabalhar com snapshots \(p. 1153\)](#)
- [Executar instâncias \(RunInstances\) \(p. 1161\)](#)
- [Trabalhar com Instâncias spot \(p. 1172\)](#)
- [Exemplo: trabalhar com Instâncias reservadas \(p. 1177\)](#)
- [Exemplo: marcar recursos \(p. 1178\)](#)
- [Exemplo: trabalhar com funções do IAM \(p. 1179\)](#)
- [Exemplo: trabalhar com tabelas de rotas \(p. 1181\)](#)
- [Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS \(p. 1181\)](#)
- [Exemplo: trabalhar com modelos de execução \(p. 1182\)](#)
- [Trabalhar com metadados de instância \(p. 1182\)](#)

Exemplo: acesso somente leitura

A política a seguir concede aos usuários permissões para utilizar todas as ações da API do Amazon EC2 cujos nomes começam com `Describe`. O elemento `Resource` usa um caractere curinga para indicar que os usuários podem especificar todos os recursos com essas ações da API. O caractere curinga `*` também é necessário em casos onde a ação da API não é compatível com as permissões em nível de recurso. Para obter mais informações sobre quais ARNs você pode usar com quais ações de API do Amazon EC2, consulte [Ações, recursos e chaves de condição do Amazon EC2](#) no .

Os usuários não têm permissão para executar nenhuma ação nos recursos (a menos que outra declaração conceda a eles permissão para fazer isso) porque, por padrão, a permissão para usar ações da API é negada para os usuários.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:Describe*",  
            "Resource": "*"  
        }  
    ]  
}
```

Exemplo: restringir acesso a uma região específica

A política a seguir nega permissão aos usuários para uso de todas as ações da API do Amazon EC2 a menos que a região seja a Europa (Frankfurt). Ela usa a chave de condição global `aws:RequestedRegion`, que é compatível com todas as ações da API do Amazon EC2.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "aws:RequestedRegion": "  
                    !in [\"eu-central-1\", \"us-east-1\"]  
                "  
            }  
        }  
    ]  
}
```

```
        "Condition": {
            "StringNotEquals": {
                "aws:RequestedRegion": "eu-central-1"
            }
        }
    }
}
```

Como alternativa, você pode usar a chave de condição `ec2:Region`, que é específica ao Amazon EC2 e é compatível com todas as ações da API do Amazon EC2.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "ec2:*",  
            "Resource": "*",  
            "Condition": {  
                "StringNotEquals": {  
                    "ec2:Region": "eu-central-1"  
                }  
            }  
        }  
    ]  
}
```

Trabalhar com instâncias

Exemplos

- Exemplo: descrever, executar, interromper, iniciar e encerrar todas as instâncias (p. 1149)
 - Exemplo: descrever todas as instâncias e interromper, iniciar e encerrar somente instâncias específicas (p. 1150)

Exemplo: descrever, executar, interromper, iniciar e encerrar todas as instâncias

A política a seguir concede aos usuários permissões para utilizar as ações da API especificadas no elemento `Action`. O elemento `Resource` usa um caractere curinga `*` para indicar que os usuários podem especificar todos os recursos com essas ações da API. O caractere curinga `*` também é necessário em casos onde a ação da API não é compatível com as permissões em nível de recurso. Para obter mais informações sobre quais ARNs você pode usar com quais ações de API do Amazon EC2, consulte [Ações, recursos e chaves de condição do Amazon EC2](#) no .

Os usuários não têm permissão para usar qualquer outra ação da API (a menos que outra declaração conceda a eles permissão para fazer isso) porque, por padrão, a permissão para usar ações da API são negadas para os usuários.

```
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
    ],
    "Resource": "*"
}
]
```

Exemplo: descrever todas as instâncias e interromper, iniciar e encerrar somente instâncias específicas

A política a seguir permite que os usuários descrevam todas as instâncias, iniciem e parem somente as instâncias i-1234567890abcdef0 e i-0598c7d356eba48d7 e encerrem somente instâncias em Leste dos EUA (Norte da Virgínia) Região (us-east-1) com a tag de recurso "purpose=test".

A primeira declaração usa um caractere curinga * para o elemento Resource para indicar que os usuários podem especificar todos os recursos com a ação. Nesse caso, os usuários podem listar todas as instâncias. O caractere curinga * também é necessário em casos onde a ação da API não é compatível com permissões em nível de recurso (nesse caso, ec2:DescribeInstances). Para obter mais informações sobre quais ARNs você pode usar com quais ações de API do Amazon EC2, consulte [Ações, recursos e chaves de condição do Amazon EC2](#) no .

A segunda declaração usa permissões em nível de recurso para as ações StopInstances e StartInstances. As instâncias específicas são indicadas por seus ARNs no elemento Resource.

A terceira instrução permite que os usuários encerrem todas as instâncias na região Leste dos EUA (Norte da Virgínia) (us-east-1) que pertencem à conta da AWS especificada, mas somente quando a instância tiver a tag "purpose=test". O elemento Condition qualifica quando a declaração de política está em vigor.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StopInstances",
                "ec2:StartInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0",
                "arn:aws:ec2:us-east-1:123456789012:instance/i-0598c7d356eba48d7"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:TerminateInstances",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/purpose": "test"
                }
            }
        }
    ]
}
```

```
    ]  
}
```

Trabalhar com volumes

Exemplos

- [Exemplo: anexar e desanexar volumes \(p. 1151\)](#)
- [Exemplo: criar um volume \(p. 1151\)](#)
- [Exemplo: criar um volume com tags \(p. 1152\)](#)

Exemplo: anexar e desanexar volumes

Quando uma ação da API exige que um chamador especifique vários recursos, você deve criar uma declaração de política que permita que os usuários acessem todos os recursos necessários. Se você precisar usar um elemento `Condition` com um ou mais desses recursos, deverá criar várias declarações conforme mostrado neste exemplo.

As políticas a seguir permitem que os usuários anexem volumes com a tag "volume_user=iam-user-name" a instâncias com a tag "department=dev" e desanexem esses volumes dessas instâncias. Se você anexar essa política a um grupo do IAM, a variável da política `aws:username` fornecerá a cada usuário do IAM no grupo permissão para anexar e desanexar volumes das instâncias com uma tag chamada `volume_user` que tem o nome do usuário do IAM como um valor.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:AttachVolume",  
                "ec2:DetachVolume"  
            ],  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/department": "dev"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:AttachVolume",  
                "ec2:DetachVolume"  
            ],  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/volume_user": "${aws:username}"  
                }  
            }  
        }  
    ]  
}
```

Exemplo: criar um volume

A política a seguir permite que os usuários usem a ação da API `CreateVolume`. O usuário terá permissão para criar um volume somente se o volume for criptografado e se seu tamanho for menor que 20 GiB.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateVolume"  
            ],  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",  
            "Condition":{  
                "NumericLessThan": {  
                    "ec2:VolumeSize" : "20"  
                },  
                "Bool":{  
                    "ec2:Encrypted" : "true"  
                }  
            }  
        }  
    ]  
}
```

Exemplo: criar um volume com tags

As política a seguir inclui a chave de condição `aws:RequestTag` que requer que os usuários marquem todos os volumes que criarem com as tags `costcenter=115` e `stack=prod`. A chave de condição `aws:TagKeys` usa o modificador `ForAllValues` para indicar que somente as chaves `costcenter` e `stack` são permitidas na solicitação (nenhuma outra tag pode ser especificada). Se os usuários não passarem essas tags específicas ou não especificarem nenhuma tag, haverá talha na solicitação.

Para ações de criação de recursos que aplicam tags, os usuários também devem ter permissões para usar a ação `CreateTags`. A segunda declaração usa a chave de condição `ec2:CreateAction` para permitir que os usuários criem tags somente no contexto de `CreateVolume`. Os usuários não podem marcar volumes existentes ou quaisquer outros recursos. Para obter mais informações, consulte [Conceder permissão para marcar recursos durante a criação \(p. 1145\)](#).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowCreateTaggedVolumes",  
            "Effect": "Allow",  
            "Action": "ec2:CreateVolume",  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/costcenter": "115",  
                    "aws:RequestTag/stack": "prod"  
                },  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": ["costcenter", "stack"]  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateTags"  
            ],  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:CreateAction" : "CreateVolume"  
                }  
            }  
        }  
    ]  
}
```

```
        }
    }
}
```

A política a seguir permite que os usuários criem um volume sem precisar especificar tags. A ação `CreateTags` só será avaliada se as tags forem especificadas na solicitação `CreateVolume`. Se os usuários especificam tags, a tag deverá ser `purpose=test`. Nenhuma outra tag é permitida na solicitação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVolume",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:1234567890:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "test",
                    "ec2:CreateAction" : "CreateVolume"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "purpose"
                }
            }
        }
    ]
}
```

Trabalhar com snapshots

Veja a seguir exemplos de políticas para `CreateSnapshot` (snapshot point-in-time de um volume do EBS) e `CreateSnapshots` (snapshots de vários volumes).

Exemplos

- [Exemplo: criar um snapshot \(p. 1153\)](#)
- [Exemplo: criar snapshots \(p. 1154\)](#)
- [Exemplo: criar um snapshot com tags \(p. 1154\)](#)
- [Exemplo: criar snapshots com tags \(p. 1155\)](#)
- [Exemplo: Copiar snapshots \(p. 1160\)](#)
- [Exemplo: modificar configurações de permissão para snapshots \(p. 1160\)](#)

Exemplo: criar um snapshot

A política a seguir permite que os clientes usem a ação da API `CreateSnapshot`. O cliente poderá criar snapshots somente se o volume for criptografado e se seu tamanho for menor que 20 GiB.

```
{
    "Version": "2012-10-17",
```

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": "ec2:CreateSnapshot",
        "Resource": "arn:aws:ec2:us-east-1::snapshot/*"
    },
    {
        "Effect": "Allow",
        "Action": "ec2:CreateSnapshot",
        "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
        "Condition": {
            "NumericLessThan": {
                "ec2:VolumeSize": "20"
            },
            "Bool": {
                "ec2:Encrypted": "true"
            }
        }
    }
]
```

Exemplo: criar snapshots

A política a seguir permite que os clientes usem a ação da API [CreateSnapshots](#). O cliente só poderá criar snapshots se todos os volumes da instância forem do tipo GP2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": [
                "arn:aws:ec2:us-east-1::snapshot/*",
                "arn:aws:ec2:/*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSnapshots",
            "Resource": "arn:aws:ec2:us-east-1:/*:volume/*",
            "Condition": {
                "StringLikeIfExists": {
                    "ec2:VolumeType": "gp2"
                }
            }
        }
    ]
}
```

Exemplo: criar um snapshot com tags

A política a seguir inclui a chave de condição `aws:RequestTag` que requer que o cliente aplique as tags `costcenter=115` e `stack=prod` a todos os novos snapshots. A chave de condição `aws:TagKeys` usa o modificador `ForAllValues` para indicar que somente as chaves `costcenter` e `stack` podem ser especificadas na solicitação. A solicitação falhará se qualquer uma destas condições não for atendida.

Para ações de criação de recursos que aplicam tags, os clientes também devem ter permissões para usar a ação `CreateTags`. A terceira declaração usa a chave de condição `ec2:CreateAction` para permitir que os clientes criem tags somente no contexto de `CreateSnapshot`. Os clientes não podem marcar

volumes existentes nem quaisquer outros recursos. Para obter mais informações, consulte [Conceder permissão para marcar recursos durante a criação \(p. 1145\)](#).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshot",  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*"  
        },  
        {  
            "Sid": "AllowCreateTaggedSnapshots",  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshot",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/costcenter": "115",  
                    "aws:RequestTag/stack": "prod"  
                },  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": [  
                        "costcenter",  
                        "stack"  
                    ]  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateTags",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:CreateAction": "CreateSnapshot"  
                }  
            }  
        }  
    ]  
}
```

Exemplo: criar snapshots com tags

A política a seguir inclui a chave de condição `aws:RequestTag` que requer que o cliente aplique as tags `costcenter=115` e `stack=prod` a todos os novos snapshots. A chave de condição `aws:TagKeys` usa o modificador `ForAllValues` para indicar que somente as chaves `costcenter` e `stack` podem ser especificadas na solicitação. A solicitação falhará se qualquer uma destas condições não for atendida.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshots",  
            "Resource": [  
                "arn:aws:ec2:us-east-1::snapshot/*",  
                "arn:aws:ec2:/*::instance/*",  
                "arn:aws:ec2:/*::volume/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateTags",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/costcenter": "115",  
                    "aws:RequestTag/stack": "prod"  
                },  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": [  
                        "costcenter",  
                        "stack"  
                    ]  
                }  
            }  
        }  
    ]  
}
```

```
"Sid":"AllowCreateTaggedSnapshots",
"Effect":"Allow",
>Action":"ec2:CreateSnapshots",
"Resource":"arn:aws:ec2:us-east-1::snapshot/*",
"Condition":{

    "StringEquals":{

        "aws:RequestTag/costcenter":"115",
        "aws:RequestTag/stack":"prod"
    },
    "ForAllValues:StringEquals":{

        "aws:TagKeys":[
            "costcenter",
            "stack"
        ]
    }
},
{
    "Effect":"Allow",
    "Action":"ec2:CreateTags",
    "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
    "Condition":{

        "StringEquals":{

            "ec2:CreateAction":"CreateSnapshots"
        }
    }
}
]
```

A política a seguir permite que os clientes criem um snapshot sem precisar especificar tags. A ação `CreateTags` só será avaliada se as tags forem especificadas na solicitação `CreateSnapshot` ou `CreateSnapshots`. Se uma tag for especificada, ela deverá ser `purpose=test`. Nenhuma outra tag é permitida na solicitação.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect":"Allow",
            "Action":"ec2:CreateSnapshot",
            "Resource":"*"
        },
        {
            "Effect":"Allow",
            "Action":"ec2:CreateTags",
            "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
            "Condition":{

                "StringEquals":{

                    "aws:RequestTag/purpose":"test",
                    "ec2:CreateAction":"CreateSnapshot"
                },
                "ForAllValues:StringEquals":{

                    "aws:TagKeys":"purpose"
                }
            }
        }
    ]
}
```

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
{  
    "Effect": "Allow",  
    "Action": "ec2:CreateSnapshots",  
    "Resource": "*"  
,  
{  
    "Effect": "Allow",  
    "Action": "ec2:CreateTags",  
    "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
    "Condition": {  
        "StringEquals": {  
            "aws:RequestTag/purpose": "test",  
            "ec2:CreateAction": "CreateSnapshots"  
        },  
        "ForAllValues:StringEquals": {  
            "aws:TagKeys": "purpose"  
        }  
    }  
}  
]  
}
```

As seguintes políticas só permitirão que snapshots sejam criados se o volume de origem for marcado com `User:username` para o cliente, e o snapshot em si for marcado com `Environment:Dev` e `User:username`. O cliente pode adicionar outras tags ao snapshot.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshot",  
            "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/User": "${aws:username}"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateSnapshot",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:RequestTag/Environment": "Dev",  
                    "aws:RequestTag/User": "${aws:username}"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateTags",  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*"  
        }  
    ]  
}
```

A seguinte política de `CreateSnapshots` só permitirá que snapshots sejam criados se o volume de origem for marcado com `User:username` para o cliente e o snapshot em si for marcado com `Environment:Dev` e `User:username`.

```
{
```

```
"Version":"2012-10-17",
"Statement": [
    {
        "Effect":"Allow",
        "Action":"ec2:CreateSnapshots",
        "Resource":"arn:aws:ec2:us-east-1::*:instance/*",
    },
    {
        "Effect":"Allow",
        "Action":"ec2:CreateSnapshots",
        "Resource":"arn:aws:ec2:us-east-1:123456789012:volume/*",
        "Condition":{
            "StringEquals":{
                "ec2:ResourceTag/User":"${aws:username}"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":"ec2:CreateSnapshots",
        "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
        "Condition":{
            "StringEquals":{
                "aws:RequestTag/Environment":"Dev",
                "aws:RequestTag/User":"${aws:username}"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":"ec2:CreateTags",
        "Resource":"arn:aws:ec2:us-east-1::snapshot/*"
    }
]
```

A seguinte política só permitirá a exclusão de um snapshot se ele for marcado com o Usuário:usuário para o cliente.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect":"Allow",
            "Action":"ec2>DeleteSnapshot",
            "Resource":"arn:aws:ec2:us-east-1::snapshot/*",
            "Condition":{
                "StringEquals":{
                    "ec2:ResourceTag/User":"${aws:username}"
                }
            }
        }
    ]
}
```

A seguinte política permite que um cliente crie um snapshot mas negará a ação se o snapshot que está sendo criado tiver uma chave de tag value=stack.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect":"Allow",

```

```
"Action": [
    "ec2:CreateSnapshot",
    "ec2:CreateTags"
],
"Resource": "*"
},
{
    "Effect": "Deny",
    "Action": "ec2:CreateSnapshot",
    "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": "stack"
        }
    }
}
]
```

A seguinte política permite que um cliente crie snapshots, mas negará a ação se o snapshot que está sendo criado tiver uma chave de tag value=stack.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateSnapshots",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "stack"
                }
            }
        }
    ]
}
```

A política a seguir permite combinar várias ações em uma única política. Você só pode criar um snapshot (no contexto de CreateSnapshots) quando o snapshot é criado na região us-east-1. Você só pode criar snapshots (no contexto de CreateSnapshots) quando os snapshots são criados na região us-east-1 e quando o tipo de instância é t2*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots",
                "ec2:CreateSnapshot",
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::instance/*",
                "arn:aws:ec2:us-east-1::snapshot/*"
            ]
        }
    ]
}
```

```
        "arn:aws:ec2::*:snapshot/*",
        "arn:aws:ec2::*:volume/*"
    ],
    "Condition": {
        "StringEqualsIgnoreCase": {
            "ec2:Region": "us-east-1"
        },
        "StringLikeIfExists": {
            "ec2:InstanceType": ["t2.*"]
        }
    }
}
]
```

Exemplo: Copiar snapshots

As permissões no nível do recurso especificadas para a ação CopySnapshot (Copiar snapshot) se aplicam somente ao novo snapshot. Elas não podem ser especificadas para o snapshot de origem.

A política de exemplo a seguir permite que as entidades copiem snapshots somente se o novo snapshot for criado com a chave de tag de *purpose* e um valor de tag de *production* (*purpose=production*).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCopySnapshotWithTags",
            "Effect": "Allow",
            "Action": "ec2:CopySnapshot",
            "Resource": "arn:aws:ec2::123456789012:snapshot/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "production"
                }
            }
        }
    ]
}
```

Exemplo: modificar configurações de permissão para snapshots

A política a seguir só permite a modificação de um snapshot se ele for marcado com *User:username*, em que *username* (nome de usuário) é o nome de usuário da conta da AWS do cliente. A solicitação falhará se essa condição não for atendida.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2: ModifySnapshotAttribute",
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/user-name": "${aws:username}"
                }
            }
        }
    ]
}
```

Executar instâncias (RunInstances)

A ação da API [RunInstances](#) inicia uma ou mais Instâncias on-demand ou uma ou mais Instâncias spot. RunInstances requer uma AMI e cria uma instância. Os usuários podem especificar um par de chaves e um grupo de segurança na solicitação. A inicialização em uma VPC requer uma sub-rede, e cria uma interface de rede. A inicialização de uma AMI com suporte do Amazon EBS cria um volume. Portanto, o usuário deve ter permissões para usar esses recursos do Amazon EC2. Você pode criar um declaração de política que exija que os usuários especifiquem um parâmetro opcional em RunInstances ou restringir os usuários a valores específicos para um parâmetro.

Para obter mais informações sobre as permissões em nível de recurso que são necessárias para executar uma instância, consulte [Ações, recursos e chaves de condição do Amazon EC2 no .](#)

Observe que, por padrão, os usuários não têm permissões para descrever, iniciar, interromper ou encerrar as instâncias resultantes. Uma maneira de conceder aos usuários permissão para gerenciar as instâncias resultantes é criar uma tag específica para cada instância e criar uma declaração que permita que eles gerenciem instâncias com aquela tag. Para obter mais informações, consulte [Trabalhar com instâncias \(p. 1149\).](#)

Recursos

- [AMIs \(p. 1161\)](#)
- [Tipos de instância \(p. 1162\)](#)
- [Subnets \(p. 1163\)](#)
- [Volumes do EBS \(p. 1164\)](#)
- [Tags \(p. 1165\)](#)
- [Tags em um modelo de execução \(p. 1169\)](#)
- [GPUs elásticas \(p. 1169\)](#)
- [Modelos de execução \(p. 1170\)](#)

AMIs

A política a seguir permite que os usuários iniciem instâncias usando apenas as AMIs especificadas, `ami-9e1670f7` e `ami-45cf5c3c`. Os usuários não podem executar uma instância usando outras AMIs (a menos que outra declaração conceda permissão para os usuários fazerem isso).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": [  
                "arn:aws:ec2:region::image/ami-9e1670f7",  
                "arn:aws:ec2:region::image/ami-45cf5c3c",  
                "arn:aws:ec2:region:account:instance/*",  
                "arn:aws:ec2:region:account:volume/*",  
                "arn:aws:ec2:region:account:key-pair/*",  
                "arn:aws:ec2:region:account:security-group/*",  
                "arn:aws:ec2:region:account:subnet/*",  
                "arn:aws:ec2:region:account:network-interface/*"  
            ]  
        }  
    ]  
}
```

Como alternativa, a política a seguir permite que os usuários executem instâncias em todas as AMIs de propriedade da Amazon. O elemento `Condition` da primeira declaração testa se `ec2:Owner` é `amazon`.

Os usuários não podem executar uma instância usando outras AMIs (a menos que outra declaração conceda permissão para os usuários fazerem isso).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": [  
                "arn:aws:ec2:region::image/ami-*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Owner": "amazon"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": [  
                "arn:aws:ec2:region:account:instance/*",  
                "arn:aws:ec2:region:account:subnet/*",  
                "arn:aws:ec2:region:account:volume/*",  
                "arn:aws:ec2:region:account:network-interface/*",  
                "arn:aws:ec2:region:account:key-pair/*",  
                "arn:aws:ec2:region:account:security-group/*"  
            ]  
        }  
    ]  
}
```

Tipos de instância

A política a seguir permite que os usuários executem instâncias usando somente o tipo de instância t2.micro ou t2.small, o que você pode fazer para controlar os custos. Os usuários não podem executar instâncias maiores porque o elemento Condition da primeira declaração testa se ec2:InstanceType é t2.micro ou t2.small.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": [  
                "arn:aws:ec2:region:account:instance/*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "ec2:InstanceType": ["t2.micro", "t2.small"]  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": [  
                "arn:aws:ec2:region::image/ami-*",  
                "arn:aws:ec2:region:account:subnet/*",  
                "arn:aws:ec2:region:account:network-interface/*",  
                "arn:aws:ec2:region:account:volume/*",  
                "arn:aws:ec2:region:account:volume/*"  
            ]  
        }  
    ]  
}
```

```
        "arn:aws:ec2:region:account:key-pair/*",
        "arn:aws:ec2:region:account:security-group/*"
    ]
}
]
```

Se desejar, você pode criar uma política que negue aos usuários permissões para executar qualquer instância, com exceção dos tipos de instância `t2.micro` e `t2.small`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region:account:instance/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:InstanceType": ["t2.micro", "t2.small"]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region::image/ami-*",
                "arn:aws:ec2:region:account:network-interface/*",
                "arn:aws:ec2:region:account:instance/*",
                "arn:aws:ec2:region:account:subnet/*",
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region:account:key-pair/*",
                "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

Subnets

A política a seguir permite que os usuários executem instâncias usando apenas a sub-rede especificada, `subnet-12345678`. O grupo não pode executar instâncias em outra sub-rede (a menos que outra declaração conceda permissão para os usuários fazerem isso).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region:account:subnet/subnet-12345678",
                "arn:aws:ec2:region:account:network-interface/*",
                "arn:aws:ec2:region:account:instance/*",
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region::image/ami-*",
                "arn:aws:ec2:region:account:key-pair/*",
                "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

```
    ]
}
```

Se desejar, você pode criar uma política que negue aos usuários permissões para executar uma instância em qualquer outra sub-rede. A declaração faz isso negando permissão para criar uma interface de rede, exceto quando a sub-rede subnet-12345678 for especificada. Essa negação substitui qualquer outra política criada para permitir a execução de instâncias em outras sub-redes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region:account:network-interface/*"
            ],
            "Condition": {
                "ArnNotEquals": {
                    "ec2:Subnet": "arn:aws:ec2:region:account:subnet/subnet-12345678"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region::image/ami-*",
                "arn:aws:ec2:region:account:network-interface/*",
                "arn:aws:ec2:region:account:instance/*",
                "arn:aws:ec2:region:account:subnet/*",
                "arn:aws:ec2:region:account:volume/*",
                "arn:aws:ec2:region:account:key-pair/*",
                "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

Volumes do EBS

A política a seguir permite que os usuários executem instâncias somente se os volumes do EBS para a instância estiverem criptografados. O usuário deve executar uma instância em uma AMI criada com snapshots criptografados, para garantir que o volume raiz esteja criptografado. Qualquer volume adicional que o usuário anexe à instância durante a execução também deve estar criptografado.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region::volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:region::volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "false"
                }
            }
        }
    ]
}
```

```
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": [
            "arn:aws:ec2::::image/ami-*",
            "arn:aws:ec2::::network-interface/*",
            "arn:aws:ec2::::instance/*",
            "arn:aws:ec2::::subnet/*",
            "arn:aws:ec2::::key-pair/*",
            "arn:aws:ec2::::security-group/*"
        ]
    }
}
```

Tags

Marque instâncias na criação

A política a seguir permite que os usuários executem instâncias e as marquem durante a criação. Para ações de criação de recursos que aplicam tags, os usuários devem ter permissões para usar a ação `CreateTags`. A segunda declaração usa a chave de condição `ec2:CreateAction` para permitir que os usuários criem tags somente no contexto de `RunInstances` e somente para instâncias. Os usuários não podem marcar recursos existentes e não podem marcar volumes usando a solicitação `RunInstances`.

Para obter mais informações, consulte [Conceder permissão para marcar recursos durante a criação \(p. 1145\)](#).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction" : "RunInstances"
                }
            }
        }
    ]
}
```

Marque instâncias e volumes na criação com tags específicas

As política a seguir inclui a chave de condição `aws:RequestTag` que requer que os usuários marquem todas as instâncias e os volumes criados por `RunInstances` com as tags `environment=production` e `purpose=webserver`. A chave de condição `aws:TagKeys` usa o modificador `ForAllValues` para indicar que somente as chaves `environment` e `purpose` são permitidas na solicitação (nenhuma outra tag pode ser especificada). Se nenhuma tag for especificada na solicitação, haverá falha na solicitação.

```
{
    "Version": "2012-10-17",
```

```
"Statement": [
{
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances"
    ],
    "Resource": [
        "arn:aws:ec2:region::image/*",
        "arn:aws:ec2:region:account:subnet/*",
        "arn:aws:ec2:region:account:network-interface/*",
        "arn:aws:ec2:region:account:security-group/*",
        "arn:aws:ec2:region:account:key-pair/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances"
    ],
    "Resource": [
        "arn:aws:ec2:region:account:volume/*",
        "arn:aws:ec2:region:account:instance/*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/environment": "production" ,
            "aws:RequestTag/purpose": "webserver"
        },
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["environment", "purpose"]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:region:account:/*/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
        }
    }
}
]
```

Marque instâncias e volumes na criação com pelo menos uma tag específica

A política a seguir usa o modificador `ForAnyValue` na condição `aws:TagKeys` para indicar que pelo menos uma tag deve ser especificada na solicitação e deve conter a chave `environment` ou `webserver`. A tag deve ser aplicada a instâncias e a volumes. Qualquer valor de tag pode ser especificado na solicitação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [

```

```
"arn:aws:ec2:region::image/*",
"arn:aws:ec2:region:account:subnet/*",
"arn:aws:ec2:region:account:network-interface/*",
"arn:aws:ec2:region:account:security-group/*",
"arn:aws:ec2:region:account:key-pair/*"
],
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances"
    ],
    "Resource": [
        "arn:aws:ec2:region:account:volume/*",
        "arn:aws:ec2:region:account:instance/*"
    ],
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:TagKeys": ["environment", "webserver"]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": "arn:aws:ec2:region:account:/*/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction" : "RunInstances"
        }
    }
}
]
```

Se forem marcadas na criação, as instâncias deverão ser marcadas com uma tag específica

Na política a seguir, os usuários não precisam especificar tags na solicitação, mas se o fizerem, a tag deverá ser `purpose=test`. Nenhuma outra tag é permitida. Os usuários podem aplicar as tags a qualquer recurso marcável na solicitação `RunInstances`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account:/*/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/purpose": "test",
                    "ec2:CreateAction" : "RunInstances"
                }
            }
        }
    ]
}
```

```
        "ForAllValues:StringEquals": {
            "aws:TagKeys": "purpose"
        }
    }
}
```

Para não permitir que ninguém adicione tags na criação para RunInstances

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1::subnet/*",
                "arn:aws:ec2:us-east-1::network-interface/*",
                "arn:aws:ec2:us-east-1::security-group/*",
                "arn:aws:ec2:us-east-1::key-pair/*",
                "arn:aws:ec2:us-east-1::volume/*",
                "arn:aws:ec2:us-east-1::instance/*",
                "arn:aws:ec2:us-east-1::spot-instances-request/*"
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Permitir apenas tags específicas para spot-instances-request. A inconsistência surpresa número 2 entra em jogo aqui. Em circunstâncias normais, não especificar tag alguma resultará em Não autenticado. No caso de spot-instances-request, esta política não será avaliada se não houver tags spot-instances-request, portanto, uma solicitação Spot on Run sem tag será bem-sucedida.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1::subnet/*",
                "arn:aws:ec2:us-east-1::network-interface/*",
                "arn:aws:ec2:us-east-1::security-group/*",
                "arn:aws:ec2:us-east-1::key-pair/*",
                "arn:aws:ec2:us-east-1::volume/*",
                "arn:aws:ec2:us-east-1::instance/*",
                "arn:aws:ec2:us-east-1::spot-instances-request/*"
            ]
        }
    ]
}
```

```
        ],
    },
    {
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": "production"
            }
        }
    }
]
```

Tags em um modelo de execução

No exemplo a seguir, os usuários poderão executar instâncias, mas apenas se usarem um modelo de execução específico (lt-09477bcd97b0d310e). A chave de condição `ec2:IsLaunchTemplateResource` impede que os usuários substituam alguns recursos especificados no modelo de execução. A segunda parte da instrução permite que os usuários marquem instâncias durante a criação; essa parte da instrução será necessária se as tags forem especificadas para a instância no modelo de execução.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/
lt-09477bcd97b0d310e"
                },
                "Bool": {
                    "ec2:IsLaunchTemplateResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2>CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2>CreateAction" : "RunInstances"
                }
            }
        }
    ]
}
```

GPUs elásticas

Na política a seguir, os usuários podem executar uma instância e especificar uma GPU elástica para anexar à instância. Os usuários podem executar instâncias em qualquer região, mas só podem anexar uma GPU elástica durante uma execução na região `us-east-2`.

A chave de condição `ec2:ElasticGpuType` usa o modificador `ForAnyValue` para indicar que somente os tipos de GPU elásticas `eg1.medium` e `eg1.large` são permitidos na solicitação.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:*:account:elastic-gpu/*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Region": "us-east-2"  
                },  
                "ForAnyValue:StringLike": {  
                    "ec2:ElasticGpuType": [  
                        "eg1.medium",  
                        "eg1.large"  
                    ]  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": [  
                "arn:aws:ec2:::image/ami-*",  
                "arn:aws:ec2:::account:network-interface/*",  
                "arn:aws:ec2:::account:instance/*",  
                "arn:aws:ec2:::account:subnet/*",  
                "arn:aws:ec2:::account:volume/*",  
                "arn:aws:ec2:::account:key-pair/*",  
                "arn:aws:ec2:::account:security-group/*"  
            ]  
        }  
    ]  
}
```

Modelos de execução

No exemplo a seguir, os usuários poderão executar instâncias, mas apenas se usarem um modelo de execução específico (`lt-09477bcd97b0d310e`). Os usuários podem substituir quaisquer parâmetros no modelo de execução especificando os parâmetros na ação `RunInstances`.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": "*",  
            "Condition": {  
                "ArnLike": {  
                    "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/  
lt-09477bcd97b0d310e"  
                }  
            }  
        }  
    ]  
}
```

}

Neste exemplo, os usuários poderão executar instâncias apenas se usarem um modelo de execução. A política usa a chave de condição `ec2: IsLaunchTemplateResource` para impedir que os usuários substituam os ARNs pré-existentes no modelo de execução.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": "*",  
            "Condition": {  
                "ArnLike": {  
                    "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/*"  
                },  
                "Bool": {  
                    "ec2:IsLaunchTemplateResource": "true"  
                }  
            }  
        }  
    ]  
}
```

No exemplo a seguir, a política permitirá que o usuário execute instâncias, mas apenas se usarem um modelo de execução. Os usuários não podem substituir os parâmetros de interface de rede e sub-rede na solicitação; esses parâmetros só podem ser especificados no modelo de execução. A primeira parte da instrução usa o elemento `NotResource` para permitir todos os outros recursos, exceto interfaces de rede e sub-redes. A segunda parte da instrução permite recursos de interface de rede e sub-rede, mas somente se eles forem originários do modelo de execução.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "NotResource": [ "arn:aws:ec2:region:account:subnet/*",  
                            "arn:aws:ec2:region:account:network-interface/*" ],  
            "Condition": {  
                "ArnLike": {  
                    "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/*"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": [ "arn:aws:ec2:region:account:subnet/*",  
                         "arn:aws:ec2:region:account:network-interface/*" ],  
            "Condition": {  
                "ArnLike": {  
                    "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/*"  
                },  
                "Bool": {  
                    "ec2:IsLaunchTemplateResource": "true"  
                }  
            }  
        }  
    ]  
}
```

O exemplo a seguir permitirá que os usuários executem instâncias somente se usarem um modelo de execução, e somente se o modelo de execução tiver a tag `Purpose=Webservers`. Os usuários não podem substituir nenhum dos parâmetros do modelo de execução na ação `RunInstances`.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "NotResource": "arn:aws:ec2:region:account:launch-template/*",  
            "Condition": {  
                "ArnLike": {  
                    "ec2:LaunchTemplate": "arn:aws:ec2:region:account:launch-template/*"  
                },  
                "Bool": {  
                    "ec2:IsLaunchTemplateResource": "true"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:RunInstances",  
            "Resource": "arn:aws:ec2:region:account:launch-template/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/Purpose": "Webservers"  
                }  
            }  
        }  
    ]  
}
```

Trabalhar com Instâncias spot

Você pode usar a ação `RunInstances` para criar solicitações de instância spot e marcar solicitações de instância spot na criação. O recurso a ser especificado para `RunInstances` é `spot-instances-request`.

O recurso `spot-instances-request` é avaliado na política do IAM da seguinte forma:

- Se você não marcar uma solicitação de instância spot na criação, o Amazon EC2 não avaliará o recurso `spot-instances-request` na instrução `RunInstances`.
- Se você marcar uma solicitação de instância spot na criação, o Amazon EC2 avaliará o recurso `spot-instances-request` na instrução `RunInstances`.

Portanto, para o recurso `spot-instances-request`, as seguintes regras se aplicam à diretiva do IAM:

- Caso você use `RunInstances` para criar uma solicitação de instância spot e não pretenda marcar a solicitação de instância spot na criação, não será necessário permitir explicitamente o recurso `spot-instances-request`. A chamada será bem-sucedida.
- Caso use `RunInstances` para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, você deverá incluir o recurso `spot-instances-request` na instrução de permissão `RunInstances`, caso contrário, a chamada falhará.
- Caso você use `RunInstances` para criar uma solicitação de instância spot e pretenda marcar a solicitação de instância spot na criação, especifique o recurso `spot-instances-request` ou um curinga * na instrução de permissão `CreateTags`, caso contrário, a chamada falhará.

Você pode solicitar Instâncias spot usando `RunInstances` ou `RequestSpotInstances`. Os exemplos de políticas do IAM a seguir se aplicam somente ao solicitar Instâncias spot usando `RunInstances`.

Exemplo: solicitar Instâncias spot usando RunInstances

A política a seguir permite que os usuários solicitem Instâncias spot usando a ação RunInstances. O recurso `spot-instances-request`, que é criado por RunInstances, solicita Instâncias spot.

Note

Para usar RunInstances a fim de criar solicitações de instância spot, você pode omitir `spot-instances-request` da lista Resource caso pretenda marcar as solicitações de instância spot na criação. Isso ocorre porque o Amazon EC2 não avalia o recurso `spot-instances-request` na instrução RunInstances se a solicitação de instância spot não estiver marcada na criação.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowRun",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:us-east-1::image/*",  
                "arn:aws:ec2:us-east-1::subnet/*",  
                "arn:aws:ec2:us-east-1::network-interface/*",  
                "arn:aws:ec2:us-east-1::security-group/*",  
                "arn:aws:ec2:us-east-1::key-pair/*",  
                "arn:aws:ec2:us-east-1::volume/*",  
                "arn:aws:ec2:us-east-1::instance/*",  
                "arn:aws:ec2:us-east-1::spot-instances-request/*"  
            ]  
        }  
    ]  
}
```

Warning

NÃO COMPATÍVEL – Exemplo: negar permissão aos usuários para solicitar Instâncias spot usando RunInstances

A política a seguir não é compatível com o recurso `spot-instances-request`.

A política a seguir destina-se a conceder permissão aos usuários para iniciar Instâncias on-demand, mas negar a permissão de solicitação Instâncias spot. O recurso `spot-instances-request`, criado por RunInstances, é o recurso que solicita Instâncias spot. A segunda instrução destina-se a negar a ação RunInstances para o recurso `spot-instances-request`. No entanto, esta condição não é compatível porque o Amazon EC2 não avalia o recurso `spot-instances-request` na instrução RunInstances se a solicitação de instância spot não estiver marcada na criação.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowRun",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:us-east-1::image/*",  
                "arn:aws:ec2:us-east-1::subnet/*",  
                "arn:aws:ec2:us-east-1::network-interface/*",  
                "arn:aws:ec2:us-east-1::security-group/*",  
                "arn:aws:ec2:us-east-1::spot-instances-request/*"  
            ]  
        },  
        {  
            "Sid": "DenyRun",  
            "Effect": "Deny",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:us-east-1::spot-instances-request/*"  
            ]  
        }  
    ]  
}
```

```
        "arn:aws:ec2:us-east-1::key-pair/*",
        "arn:aws:ec2:us-east-1::volume/*",
        "arn:aws:ec2:us-east-1::instance/*"
    ],
},
{
    "Sid": "DenySpotInstancesRequests - NOT SUPPORTED - DO NOT USE!",
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:us-east-1::spot-instances-request/*"
}
]
```

Exemplo: marcar solicitações de instância spot na criação

A política a seguir permite que os usuários marquem todos os recursos criados durante o lançamento da instância. A primeira instrução permite que RunInstances crie os recursos listados. O recurso `spot-instances-request`, criado por RunInstances, é o recurso que solicita Instâncias spot. A segunda instrução fornece um curinga `*` para permitir que todos os recursos sejam marcados quando criados no momento da execução da instância.

Note

Se você marcar uma solicitação de instância spot na criação, o Amazon EC2 avaliará o recurso `spot-instances-request` na instrução `RunInstances`. Portanto, você deve permitir explicitamente o recurso `spot-instances-request` para a ação `RunInstances`, caso contrário, a chamada falhará.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1::subnet/*",
                "arn:aws:ec2:us-east-1::network-interface/*",
                "arn:aws:ec2:us-east-1::security-group/*",
                "arn:aws:ec2:us-east-1::key-pair/*",
                "arn:aws:ec2:us-east-1::volume/*",
                "arn:aws:ec2:us-east-1::instance/*",
                "arn:aws:ec2:us-east-1::spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Exemplo: negar marcações na criação para solicitações de instância spot

A política a seguir nega aos usuários a permissão para marcar os recursos criados durante a execução da instância.

A primeira instrução permite que RunInstances crie os recursos listados. O recurso `spot-instances-request`, criado por RunInstances, é o recurso que solicita Instâncias spot. A segunda instrução fornece um curinga * para evitar que todos os recursos sejam marcados, quando criados, no momento da execução da instância. Se `spot-instances-request` ou qualquer outro recurso estiver marcado na criação, a chamada RunInstances falhará.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowRun",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:us-east-1::image/*",  
                "arn:aws:ec2:us-east-1::subnet/*",  
                "arn:aws:ec2:us-east-1::network-interface/*",  
                "arn:aws:ec2:us-east-1::security-group/*",  
                "arn:aws:ec2:us-east-1::key-pair/*",  
                "arn:aws:ec2:us-east-1::volume/*",  
                "arn:aws:ec2:us-east-1::instance/*",  
                "arn:aws:ec2:us-east-1::spot-instances-request/*"  
            ]  
        },  
        {  
            "Sid": "DenyTagResources",  
            "Effect": "Deny",  
            "Action": "ec2:CreateTags",  
            "Resource": "*"  
        }  
    ]  
}
```

Warning

NÃO COMPATÍVEL – exemplo: permitir a criação de uma solicitação de instância spot apenas se lhe for atribuída uma tag específica

A política a seguir não é compatível com o recurso `spot-instances-request`.

A política a seguir destina-se a conceder permissão à RunInstances para criar uma solicitação de instância spot somente se a solicitação for marcada com uma tag específica.

A primeira instrução permite que RunInstances crie os recursos listados.

A segunda instrução destina-se a conceder permissão aos usuários para criar uma solicitação de instância spot somente se a solicitação tiver a tag `environment=production`. Se essa condição for aplicada a outros recursos criados por RunInstances, não especificar nenhuma tag gerará um erro `Unauthenticated`. No entanto, se nenhuma tag for especificada para a solicitação de instância spot, o Amazon EC2 não avaliará o recurso `spot-instances-request` na instrução RunInstances, o que resultará em solicitações de instância spot não marcadas sendo criadas pela RunInstances.

Observe que especificar outra tag, além de `environment=production`, gera um erro `Unauthenticated`, pois se um usuário marca uma solicitação de instância spot, o Amazon EC2 avalia o recurso `spot-instances-request` na instrução RunInstances.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowRun",  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances"  
            ],  
            "Resource": [  
                "arn:aws:ec2:us-east-1::image/*",  
                "arn:aws:ec2:us-east-1::subnet/*",  
                "arn:aws:ec2:us-east-1::network-interface/*",  
                "arn:aws:ec2:us-east-1::security-group/*",  
                "arn:aws:ec2:us-east-1::key-pair/*",  
                "arn:aws:ec2:us-east-1::volume/*",  
                "arn:aws:ec2:us-east-1::instance/*",  
                "arn:aws:ec2:us-east-1::spot-instances-request/*"  
            ]  
        },  
        {  
            "Sid": "DenyTagResources",  
            "Effect": "Deny",  
            "Action": "ec2:CreateTags",  
            "Resource": "*"  
        }  
    ]  
}
```

```
        "ec2:RunInstances"
    ],
    "Resource": [
        "arn:aws:ec2:us-east-1::image/*",
        "arn:aws:ec2:us-east-1::subnet/*",
        "arn:aws:ec2:us-east-1::network-interface/*",
        "arn:aws:ec2:us-east-1::security-group/*",
        "arn:aws:ec2:us-east-1::key-pair/*",
        "arn:aws:ec2:us-east-1::volume/*",
        "arn:aws:ec2:us-east-1::instance/*"
    ]
},
{
    "Sid": "RequestSpotInstancesOnlyIfTagIs_environment=production - NOT SUPPORTED - DO NOT USE!",
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:us-east-1::spot-instances-request/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/environment": "production"
        }
    }
},
{
    "Sid": "TagResources",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "*"
}

]
```

Exemplo: negar a criação de uma solicitação de instância spot se lhe for atribuída uma tag específica

A política a seguir nega à RunInstances a permissão para criar uma solicitação de instância spot se a solicitação estiver marcada com environment=production.

A primeira instrução permite que RunInstances crie os recursos listados.

A segunda instrução nega permissão aos usuários para criar uma solicitação de instância spot se a solicitação tiver a tag environment=production. Especificar environment=production como tag gerará um erro Unauthenticated. Especificar outras tags ou não especificar tags resultará na criação de uma solicitação de instância spot.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1::subnet/*",
                "arn:aws:ec2:us-east-1::network-interface/*",
                "arn:aws:ec2:us-east-1::security-group/*",
                "arn:aws:ec2:us-east-1::key-pair/*",
                "arn:aws:ec2:us-east-1::volume/*",
                "arn:aws:ec2:us-east-1::instance/*",
                "arn:aws:ec2:us-east-1::spot-instances-request/*"
            ]
        }
    ]
}
```

```
        ],
    },
    {
        "Sid": "DenySpotInstancesRequests",
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": "production"
            }
        }
    },
    {
        "Sid": "TagResources",
        "Effect": "Allow",
        "Action": "ec2:CreateTags",
        "Resource": "*"
    }
]
```

Exemplo: trabalhar com Instâncias reservadas

A política a seguir concede aos usuários permissão para exibir, modificar e comprar Instâncias reservadas na sua conta.

Não é possível definir permissões em nível de recurso para instâncias reservadas. Essa política significa que os usuários têm acesso a todas as Instâncias reservadas na conta.

O elemento Resource usa um caractere curinga * para indicar que os usuários podem especificar todos os recursos com a ação. Nesse caso, os usuários podem listar e modificar todas as Instâncias reservadas na conta. Eles também podem comprar Instâncias reservadas usando as credenciais da conta. O caractere curinga * também é necessário em casos onde a ação da API não é compatível com as permissões em nível de recurso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeReservedInstances",
                "ec2:ModifyReservedInstances",
                "ec2:PurchaseReservedInstancesOffering",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeReservedInstancesOfferings"
            ],
            "Resource": "*"
        }
    ]
}
```

Para permitir que os usuários exibam e modifiquem as Instâncias reservadas na conta, mas não comprem novas Instâncias reservadas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeReservedInstances",
                "ec2:ModifyReservedInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

```
        "Action": [
            "ec2:DescribeReservedInstances",
            "ec2:ModifyReservedInstances",
            "ec2:DescribeAvailabilityZones"
        ],
        "Resource": "*"
    }
}
```

Exemplo: marcar recursos

A política a seguir permite que os usuários usem a ação `CreateTags` para aplicar tags a uma instância somente se a tag contiver a chave `environment` e o valor `production`. O modificador `ForAllValues` é usado com a chave de condição `aws:TagKeys` para indicar que somente a chave `environment` é permitida na solicitação (nenhuma outra tag é permitida). O usuário não pode marcar nenhum outro tipo de recurso.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "environment"
                    ]
                }
            }
        }
    ]
}
```

A política a seguir permite que os usuários marquem qualquer recurso marcável que já tenha uma tag com a chave `owner` e um valor do nome de usuário do IAM. Além disso, os usuários devem especificar uma tag com uma chave de `anycompany:environment-type` e um valor de `test` ou de `prod` na solicitação. Os usuários podem especificar tags adicionais na solicitação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account:/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/anycompany:environment-type": ["test", "prod"],
                    "ec2:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

```
        }
    ]
```

Você pode criar uma política do IAM que permite que os usuários exclam tags específicas de um recurso. Por exemplo, a política a seguir permite que os usuários exclam tags de um volume se as chaves das tags especificadas na solicitação forem `environment` ou `cost-center`. Qualquer valor pode ser especificado para a tag, mas a chave da tag deve corresponder a uma das chaves especificadas.

Note

Se você excluir um recurso, todas as tags associadas ao recurso também serão excluídas. Os usuários não precisam de permissões para utilizar a ação `ec2:DeleteTags` para excluir um recurso que tenha tags. Eles precisam apenas das permissões para executar a ação de exclusão.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment", "cost-center"]
        }
      }
    }
  ]
}
```

Essa política permite que os usuários exclam somente a tag `environment=prod` em qualquer recurso e apenas se o recurso já estiver marcado com a chave `owner` e com um valor do nome de usuário do IAM. Os usuários não podem excluir nenhuma outra tag de um recurso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:region:account:/*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "ec2:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

Exemplo: trabalhar com funções do IAM

A política a seguir permite que os usuários anexem, substituam e desanexem uma função do IAM para instâncias que tenham a tag `department=test`. As substituição ou a desanexação de uma função do

IAM requer um ID de associação, portanto, a política também concede aos usuários permissão para usar a ação `ec2:DescribeIamInstanceProfileAssociations`.

Os usuários do IAM devem ter permissão para usar a ação `iam:PassRole` para passar a função para a instância.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:AssociateIamInstanceProfile",  
                "ec2:ReplaceIamInstanceProfileAssociation",  
                "ec2:DisassociateIamInstanceProfile"  
            ],  
            "Resource": "arn:aws:ec2:region:account:instance/*",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/department": "test"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:DescribeIamInstanceProfileAssociations",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "iam:PassRole",  
            "Resource": "*"  
        }  
    ]  
}
```

A política a seguir permite que os usuários anexem ou substituam uma função do IAM para qualquer instância. Os usuários podem anexar ou substituir apenas funções do IAM com nomes que começam com `TestRole-`. Para a ação `iam:PassRole`, especifique o nome da função do IAM e não o perfil da instância (se os nomes forem diferentes). Para obter mais informações, consulte [Perfis de instância \(p. 1196\)](#).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:AssociateIamInstanceProfile",  
                "ec2:ReplaceIamInstanceProfileAssociation"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:DescribeIamInstanceProfileAssociations",  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "iam:PassRole",  
            "Resource": "arn:aws:iam::account:role/TestRole-*"  
        }  
    ]  
}
```

```
    ]  
}
```

Exemplo: trabalhar com tabelas de rotas

A política a seguir permite aos usuários adicionar, remover e substituir rotas em tabelas de rotas associadas à VPC vpc-ec43eb89 somente. Para especificar uma VPC para a chave de condição ec2:Vpc, especifique o ARN total da VPC.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DeleteRoute",  
                "ec2>CreateRoute",  
                "ec2:ReplaceRoute"  
            ],  
            "Resource": [  
                "arn:aws:ec2:region:account:route-table/*"  
            ],  
            "Condition": {  
                "StringEquals": {  
                    "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-ec43eb89"  
                }  
            }  
        }  
    ]  
}
```

Exemplo: permitir que uma instância específica visualize recursos em outros serviços da AWS

O exemplo a seguir é de uma política que você pode anexar a uma função do IAM. As políticas permitem que uma instância exiba recursos em vários serviços da AWS. Ele usa a chave de condição ec2:SourceInstanceARN para especificar que a instância na qual a solicitação é feita deve ser a instância i-093452212644b0dd6. Se a mesma função do IAM estiver associada a outra instância, a outra instância não poderá executar nenhuma dessas ações.

A chave ec2:SourceInstanceARN é uma chave de condição em toda a AWS, portanto, ela pode ser usada para outras ações de serviço, não apenas para o Amazon EC2.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeVolumes",  
                "s3>ListAllMyBuckets",  
                "dynamodb>ListTables",  
                "rds:DescribeDBInstances"  
            ],  
            "Resource": [  
                "*"  
            ],  
            "Condition": {  
                "ArnEquals": {  
                    "ec2:SourceInstanceARN": "arn:aws:ec2:region:account:instance/  
i-093452212644b0dd6"  
                }  
            }  
        }  
    ]  
}
```

```
        }
    ]
}
```

Exemplo: trabalhar com modelos de execução

A política a seguir permite que os usuários criem uma versão de modelo de execução e alterem um modelo de execução, mas somente um modelo de execução específico (lt-09477bcd97b0d3abc). Os usuários não podem trabalhar com outros modelos de execução.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account:launch-template/lt-09477bcd97b0d3abc"
    }
  ]
}
```

A política a seguir permite que os usuários exclam qualquer modelo de execução e versão de modelo de execução, desde que o modelo tenha a tag `Purpose=Testing`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2>DeleteLaunchTemplate",
        "ec2>DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account:launch-template/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Trabalhar com metadados de instância

As políticas a seguir garantem que os usuários possam recuperar somente [metadados de instância \(p. 622\)](#) usando o Serviço de metadados da instância versão 2 (IMDSv2). É possível combinar as quatro políticas a seguir em uma única política com quatro instruções. Quando combinadas como uma única política, você pode usar a política como uma política de controle de serviço (SCP). Ela pode funcionar tão bem como uma política de negação aplicada a uma política existente do IAM (retirando e limitando a permissão existente) ou como uma SCP aplicada globalmente em uma conta, uma unidade organizacional (UO) ou uma organização inteira.

Note

As seguintes políticas de opções de metadados de RunInstances devem ser usadas em conjunto com uma política que concede ao principal permissões para executar uma instância com

RunInstances. Se o principal também não tiver permissões para RunInstances, não poderá executar uma instância. Para obter mais informações, consulte as políticas em [Trabalhar com instâncias \(p. 1149\)](#) e [Executar instâncias \(RunInstances\) \(p. 1161\)](#).

Important

Se você usar grupos do Auto Scaling e precisar exigir o uso do IMDSv2 em todas as novas instâncias, seus grupos do Auto Scaling deverão usar modelos de execução.

Quando um grupo do Auto Scaling usa um modelo de execução, as permissões de `ec2:RunInstances` do principal do IAM são verificadas quando um novo grupo do Auto Scaling é criado. Elas também são verificadas quando um grupo existente do Auto Scaling é atualizado para usar um novo modelo de execução ou uma nova versão de um modelo de execução.

As restrições sobre o uso do IMDSv1 em principais do IAM para RunInstances são verificadas somente quando um grupo de Auto Scaling que está usando um modelo de execução é criado ou atualizado. Para um grupo do Auto Scaling configurado para usar o modelo de execução `Latest` ou `Default`, as permissões não são verificadas quando uma nova versão do modelo de execução é criada. Para que as permissões sejam verificadas, você deve configurar o grupo do Auto Scaling para usar uma versão específica do modelo de execução.

Para impor o uso do IMDSv2 em instâncias executadas por grupos do Auto Scaling, as seguintes etapas adicionais são necessárias:

1. Desabilite o uso de configurações de execução para todas as contas em sua organização usando SCPs (service control policies - políticas de controle de serviço) ou limites de permissões do IAM para novos principais criados. Para principais existentes do IAM com permissões de grupo do Auto Scaling, atualize suas políticas associadas com essa chave de condição. Para desabilitar o uso de configurações de execução, crie ou modifique a SCP relevante, o limite de permissões ou a política do IAM com a `"autoscaling:LaunchConfigurationName"` chave de condição com o valor especificado como `null`.
2. Para novos modelos de execução, configure as opções de metadados da instância no modelo de execução. Para modelos de execução existentes, crie uma versão do modelo de execução e configure as opções de metadados da instância na nova versão.
3. Na política que concede a qualquer principal permissão para usar um modelo de execução, restrinja a associação de `$latest` e `$default` especificando `"autoscaling:LaunchTemplateVersionSpecified": "true"`. Ao restringir o uso a uma versão específica de um modelo de execução, você pode garantir que novas instâncias serão executadas usando a versão na qual as opções de metadados da instância estão configuradas. Para obter mais informações, consulte [LaunchTemplateSpecification](#) no Referência da API do Amazon EC2 Auto Scaling, especificamente o parâmetro `Version`.
4. Para um grupo do Auto Scaling que usa uma configuração de execução, substitua a configuração de execução por um modelo de execução. Para obter mais informações, consulte [Substituir uma configuração de execução por um modelo de execução](#) no Guia do usuário do Amazon EC2 Auto Scaling.
5. Para um grupo do Auto Scaling que usa um modelo de execução, certifique-se de que ele usa um novo modelo de execução com as opções de metadados da instância configuradas ou usa uma nova versão do modelo de execução atual com as opções de metadados da instância configuradas. Para obter mais informações, consulte [update-auto-scaling-group](#) na AWS CLI Command Reference (Referência de comandos da AWS CLI).

Exemplos

- [Exigir o uso de IMDSv2 \(p. 1184\)](#)
- [Especificar o limite máximo de saltos \(p. 1184\)](#)
- [Limitar quem pode modificar as opções de metadados da instância \(p. 1184\)](#)
- [Exigir que as credenciais de função sejam recuperadas de IMDSv2 \(p. 1185\)](#)

Exigir o uso de IMDSv2

A política a seguir especifica que não é possível chamar a API RunInstances a menos que a instância também esteja optada para exigir o uso de IMDSv2 (indicado por "ec2:MetadataHttpTokens": "required"). Se você não especificar que a instância requer IMDSv2, receberá um erro UnauthorizedOperation ao chamar a API RunInstances.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "RequireImdsV2",  
            "Effect": "Deny",  
            "Action": "ec2:RunInstances",  
            "Resource": "arn:aws:ec2:*:instance/*",  
            "Condition": {  
                "StringNotEquals": {  
                    "ec2:MetadataHttpTokens": "required"  
                }  
            }  
        }  
    ]  
}
```

Especificar o limite máximo de saltos

A política a seguir especifica que não é possível chamar a API RunInstances a menos que também especifique um limite de saltos, que não pode ser superior a 3. Se isso não for feito, você receberá um erro UnauthorizedOperation ao chamar a API RunInstances.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "MaxImdsHopLimit",  
            "Effect": "Deny",  
            "Action": "ec2:RunInstances",  
            "Resource": "arn:aws:ec2:*:instance/*",  
            "Condition": {  
                "NumericGreaterThanOrEqual": {  
                    "ec2:MetadataHttpPutResponseHopLimit": "3"  
                }  
            }  
        }  
    ]  
}
```

Limitar quem pode modificar as opções de metadados da instância

A política a seguir remove a capacidade da população geral de administradores de modificar opções de metadados de instância e permite que somente usuários com a função ec2-imds-admins façam alterações. Se qualquer principal diferente da função ec2-imds-admins tentar chamar a API ModifyInstanceMetadataOptions, receberá um erro UnauthorizedOperation. Essa instrução pode ser usada para controlar o uso da API ModifyInstanceMetadataOptions. No momento, não há controles de acesso refinados (condições) para a API ModifyInstanceMetadataOptions.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Principal": "ec2-imds-admins",  
            "Action": "ec2:ModifyInstanceMetadataOptions",  
            "Resource": "arn:aws:ec2:instance/*"  
        }  
    ]  
}
```

```
"Sid": "AllowOnlyImdsAdminsToModifySettings",
"Effect": "Deny",
>Action": "ec2:ModifyInstanceMetadataOptions",
"Resource": "*",
"Condition": {
    "StringNotLike": {
        "aws:PrincipalARN": "arn:aws:iam::*:role/ec2-imds-admins"
    }
}
]
```

Exigir que as credenciais de função sejam recuperadas de IMDSv2

A política a seguir especifica que, se essa política for aplicada a uma função e a função for assumida pelo serviço do EC2 e as credenciais resultantes forem usadas para assinar uma solicitação, a solicitação deverá ser assinada pelas credenciais de função do EC2 recuperadas do IMDSv2. Caso contrário, todas as suas chamadas de API receberão um erro `UnauthorizedOperation`. Essa instrução/política pode ser aplicada de modo geral porque, se a solicitação não for assinada por credenciais de função do EC2, ela não terá efeito.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Políticas de exemplo para trabalhar no console do Amazon EC2

Você pode usar as políticas do IAM para conceder permissões aos usuários para visualizarem e trabalharem com recursos específicos no console do Amazon EC2. Você pode usar os exemplos de políticas da seção anterior. No entanto, eles foram criados para solicitações feitas com a AWS CLI ou com um AWS SDK. O console usa ações de API adicionais para seus recursos, portanto, essas políticas talvez não funcionem como esperado. Por exemplo, um usuário que tem permissão para usar somente a ação da API `DescribeVolumes` encontrará erros ao tentar visualizar volumes no console. Esta seção demonstra políticas que permitem que os usuários trabalhem com partes específicas do console.

Tip

Para ajudar a descobrir quais ações de API são necessárias para realizar tarefas no console, você pode usar um serviço como o AWS CloudTrail. Para obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#). Se sua política não conceder permissão para criar ou modificar um recurso específico, o console exibirá uma mensagem codificada com informações de diagnóstico. Você pode decodificar a mensagem usando a ação de API `DecodeAuthorizationMessage` para AWS STS, ou o comando `decode-authorization-message` na AWS CLI.

Exemplos

- [Exemplo: acesso somente leitura \(p. 1186\)](#)
- [Exemplo: usar o assistente de execução do EC2 \(p. 1187\)](#)
- [Exemplo: trabalhar com volumes \(p. 1190\)](#)
- [Exemplo: trabalhar com grupos de segurança \(p. 1191\)](#)
- [Exemplo: trabalhar com endereços IP elásticos \(p. 1193\)](#)
- [Exemplo: trabalhar com Instâncias reservadas \(p. 1194\)](#)

Para obter informações adicionais sobre como criar políticas para o console do Amazon EC2, consulte a seguinte postagem do Blog de segurança da AWS: [Granting Users Permission to Work in the Amazon EC2 Console \(Conceder permissão aos usuários para trabalhar no console do Amazon EC2\)](#).

Exemplo: acesso somente leitura

Para permitir que os usuários visualizem todos os recursos no console do Amazon EC2, você pode usar a mesma política como no exemplo a seguir: [Exemplo: acesso somente leitura \(p. 1148\)](#). Os usuários não podem executar nenhuma ação nesses recursos ou criar novos recursos, a menos que outra declaração conceda permissão a eles para fazer isso.

Visualizar instâncias, AMIs e snapshots

Como alternativa, você pode fornecer acesso somente leitura a um subconjunto de recursos. Para fazer isso, substitua o caractere curinga * na ação de API `ec2:Describe` por ações `ec2:Describe` específicas para cada recurso. A política a seguir permite que os usuários visualizem todas as instâncias, AMIs e snapshots no console do Amazon EC2. A ação `ec2:DescribeTags` permite que os usuários visualizem AMIs públicas. O console requer que as informações de marcação exibam AMIs públicas. No entanto, você pode remover essa ação para permitir que os usuários visualizem somente AMIs privadas.

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeInstances",  
            "ec2:DescribeImages",  
            "ec2:DescribeTags",  
            "ec2:DescribeSnapshots"  
        ],  
        "Resource": "*"  
    }]  
}
```

Note

As ações da API `ec2:Describe*` do Amazon EC2 não oferecem suporte a permissões em nível de recurso, portanto, não é possível controlar quais recursos individuais os usuários podem visualizar no console. Portanto, o caractere curinga * é necessário no elemento `Resource` da declaração acima. Para obter mais informações sobre quais ARNs você pode usar com quais ações de API do Amazon EC2, consulte [Ações, recursos e chaves de condição do Amazon EC2 no](#).

Visualizar instâncias e métricas do CloudWatch

A política a seguir permite que os usuários visualizem instâncias no console do Amazon EC2, bem como alarmes e métricas do CloudWatch na guia Monitoring (Monitoramento) da página Instances (Instâncias). O console do Amazon EC2 usa a API do CloudWatch para exibir os alarmes e as métricas, portanto,

você deve conceder aos usuários permissão para usar as ações `cloudwatch:DescribeAlarms` e `cloudwatch:GetMetricStatistics`.

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeInstances",  
            "cloudwatch:DescribeAlarms",  
            "cloudwatch:GetMetricStatistics"  
        ],  
        "Resource": "*"  
    }]  
}
```

Exemplo: usar o assistente de execução do EC2

O assistente de execução do Amazon EC2 é uma série de telas com opções para configurar e executar uma instância. Sua política deve incluir permissão para usar as ações de API que permitem que os usuários trabalhem com as opções do assistente. Se a política não incluir a permissão para usar essas ações, alguns itens do assistente poderão não ser carregados corretamente, e os usuários não poderão concluir uma execução.

Acesso básico ao assistente de execução

Para concluir uma execução com êxito, os usuários devem receber permissão para usar a ação de API `ec2:RunInstances` e, pelo menos, as seguintes ações de API:

- `ec2:DescribeImages`: para visualizar e selecionar uma AMI.
- `ec2:DescribeInstanceTypes`: para visualizar e selecionar um tipo de instância.
- `ec2:DescribeVpcs`: para ver as opções de rede disponíveis.
- `ec2:DescribeSubnets`: para visualizar todas as sub-redes disponíveis da VPC escolhida.
- `ec2:DescribeSecurityGroups` ou `ec2>CreateSecurityGroup`: para visualizar e selecionar um grupo de segurança existente ou criar um.
- `ec2:DescribeKeyPairs` ou `ec2:CreateKeyPair`: para selecionar um par de chaves ou criar um par.
- `ec2:AuthorizeSecurityGroupIngress`: para adicionar regras de entrada.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeInstances",  
                "ec2:DescribeImages",  
                "ec2:DescribeInstanceTypes",  
                "ec2:DescribeKeyPairs",  
                "ec2:DescribeVpcs",  
                "ec2:DescribeSubnets",  
                "ec2:DescribeSecurityGroups",  
                "ec2:CreateSecurityGroup",  
                "ec2:AuthorizeSecurityGroupIngress",  
                "ec2:CreateKeyPair"  
            ],  
            "Resource": "*"  
        }]  
}
```

```
        "Resource": "*"
    },
{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": "*"
}
]
```

Você pode adicionar ações de API à sua política para fornecer mais opções aos usuários, por exemplo:

- `ec2:DescribeAvailabilityZones`: para ver e selecionar uma zona de disponibilidade específica.
- `ec2:DescribeNetworkInterfaces`: para visualizar e selecionar interfaces de rede existentes para a sub-rede selecionada.
- Para adicionar regras de saída para security groups da VPC, os usuários devem receber a permissão para usar a ação de API `ec2:AuthorizeSecurityGroupEgress`. Para modificar ou excluir regras existentes, os usuários devem receber permissão para usar a ação de API relevante `ec2:RevokeSecurityGroup*`.
- `ec2:CreateTags`: para marcar os recursos criados por `RunInstances`. Para obter mais informações, consulte [Conceder permissão para marcar recursos durante a criação \(p. 1145\)](#). Se os usuários não tiverem permissão para usar essa ação e tentarem aplicar tags na página de marcação do assistente de execução, haverá falha na execução.

Important

Tenha cuidado ao conceder aos usuários permissão para usar a ação `ec2:CreateTags`, pois isso limita sua capacidade de usar a chave de condição `ec2:ResourceTag` para restringir o uso de outros recursos. Se você conceder aos usuários permissão para usar a ação `ec2:CreateTags`, eles poderão alterar a tag de um recurso para contornar essas restrições. Para obter mais informações, consulte [Controlar o acesso aos recursos do EC2 usando tags de recursos \(p. 1147\)](#).

- Para usar parâmetros do Systems Manager ao selecionar uma AMI, você deve adicionar `ssm:DescribeParameters` e `ssm:GetParameters` à política. `ssm:DescribeParameters` concede aos usuários do IAM permissão para visualizar e selecionar parâmetros do Systems Manager. `ssm:GetParameters` concede aos usuários do IAM a permissão para obter os valores dos parâmetros do Systems Manager. Também é possível restringir o acesso a parâmetros específicos do Systems Manager. Para obter mais informações, consulte [Restringir acesso a parâmetros específicos do Systems Manager](#) posteriormente nesta seção.

Atualmente, as ações de API Amazon EC2 do `Describe*` não oferecem suporte a permissões em nível de recurso, portanto, não é possível restringir quais recursos individuais os usuários podem visualizar no assistente de execução. Contudo, você pode aplicar permissões em nível de recurso na ação de API `ec2:RunInstances` para restringir os recursos que os usuários podem usar para executar uma instância. Haverá falha na execução se os usuários selecionarem opções que não estão autorizados a usar.

Restringir o acesso a um tipo de instância, uma sub-rede e uma região específicos

A política a seguir permite que os usuários executem instâncias `t2.micro` usando AMIs de propriedade da Amazon e apenas em uma sub-rede específica (`subnet-1a2b3c4d`). Os usuários só podem executar na região `sa-east-1`. Se os usuários selecionarem outra região ou selecionarem outro tipo de instância, outra AMI ou outra sub-rede no assistente de execução, a execução falhará.

A primeira declaração concede aos usuários permissão para visualizar as opções no assistente de execução ou criar novas, conforme explicado no exemplo acima. A segunda declaração concede aos usuários permissão para usarem a interface de rede, o volume, o par de chaves, o security group e os recursos de sub-rede para a ação `ec2:RunInstances`, que são necessários para executar uma instância

em uma VPC. Para obter mais informações sobre como usar a ação `ec2:RunInstances`, consulte [Executar instâncias \(RunInstances\) \(p. 1161\)](#). A terceira e a quarta declaração concedem aos usuários permissão para usarem a instância e os recursos das AMIs respectivamente, mas somente se a instância for uma instância `t2.micro`, e somente se a AMI for de propriedade da Amazon.

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeInstances",  
            "ec2:DescribeImages",  
            "ec2:DescribeInstanceTypes",  
            "ec2:DescribeKeyPairs",  
            "ec2:CreateKeyPair",  
            "ec2:DescribeVpcs",  
            "ec2:DescribeSubnets",  
            "ec2:DescribeSecurityGroups",  
            "ec2:CreateSecurityGroup",  
            "ec2:AuthorizeSecurityGroupIngress"  
        ],  
        "Resource": "*"  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2:RunInstances",  
        "Resource": [  
            "arn:aws:ec2:sa-east-1:111122223333:network-interface/*",  
            "arn:aws:ec2:sa-east-1:111122223333:volume/*",  
            "arn:aws:ec2:sa-east-1:111122223333:key-pair/*",  
            "arn:aws:ec2:sa-east-1:111122223333:security-group/*",  
            "arn:aws:ec2:sa-east-1:111122223333:subnet/subnet-1a2b3c4d"  
        ]  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2:RunInstances",  
        "Resource": [  
            "arn:aws:ec2:sa-east-1:111122223333:instance/*"  
        ],  
        "Condition": {  
            "StringEquals": {  
                "ec2:InstanceType": "t2.micro"  
            }  
        }  
    },  
    {  
        "Effect": "Allow",  
        "Action": "ec2:RunInstances",  
        "Resource": [  
            "arn:aws:ec2:sa-east-1::image/ami-*"  
        ],  
        "Condition": {  
            "StringEquals": {  
                "ec2:Owner": "amazon"  
            }  
        }  
    }  
}
```

Restringir o acesso a parâmetros específicos do Systems Manager

A política a seguir concede acesso para usar parâmetros do Systems Manager com um nome específico.

A primeira instrução concede aos usuários permissão para visualizar parâmetros do Systems Manager ao selecionar uma AMI no assistente de inicialização. A segunda instrução concede aos usuários a permissão para usar somente parâmetros denominados prod-*.

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ssm:DescribeParameters"  
        ],  
        "Resource": "*"  
    },  
    {  
        "Effect": "Allow",  
        "Action": [  
            "ssm:GetParameters"  
        ],  
        "Resource": "arn:aws:ssm:us-east-2:123456123:parameter/prod-*"  
    }  
}
```

Exemplo: trabalhar com volumes

A política a seguir concede aos usuários permissão para visualizar e criar volumes, e para anexar e desanexar volumes em instâncias específicas.

Os usuários podem anexar um volume às instâncias que tenham a tag "purpose=test" e também desanexar volumes dessas instâncias. Para anexar um volume usando o console do Amazon EC2, é útil que os usuários tenham permissão para usar a ação ec2:DescribeInstances, pois isso permite que eles selezionem uma instância de uma lista pré-preenchida na caixa de diálogo Attach Volume (Anexar volume). No entanto, isso também permite que os usuários visualizem todas as instâncias na página Instances no console, portanto, você pode omitir essa ação.

Na primeira instrução, a ação ec2:DescribeAvailabilityZones é necessária para garantir que um usuário possa selecionar uma zona de disponibilidade ao criar um volume.

Os usuários não podem marcar os volumes que criam (durante ou após a criação do volume).

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeVolumes",  
            "ec2:DescribeAvailabilityZones",  
            "ec2>CreateVolume",  
            "ec2:DescribeInstances"  
        ],  
        "Resource": "*"  
    },  
    {  
        "Effect": "Allow",  
        "Action": [  
            "ec2:AttachVolume",  
            "ec2:DetachVolume"  
        ],  
        "Resource": "arn:aws:ec2:region:111122223333:instance/*",  
        "Condition": {  
            "StringEquals": {  
                "ec2:ResourceTag/purpose": "test"  
            }  
        }  
    }  
}
```

```
        }
    },
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": "arn:aws:ec2:region:111122223333:volume/*"
}
]
```

Exemplo: trabalhar com grupos de segurança

Visualizar grupos de segurança e adicionar e remover regras

A política a seguir concede aos usuários permissão para visualizar grupos de segurança no console do Amazon EC2, adicionar e remover regras de entrada e de saída, bem como listar e modificar descrições de regras de grupo de segurança existentes que têm a etiqueta Department=Test.

Na primeira declaração, a ação ec2:DescribeTags permite que os usuários visualizem tags no console, o que facilita a identificação dos security groups que eles têm permissão para modificar.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:ModifySecurityGroupRules",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
            ],
            "Resource": [
                "arn:aws:ec2:region:111122223333:security-group/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Department": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifySecurityGroupRules"
            ],
            "Resource": [
                "arn:aws:ec2:region:111122223333:security-group-rule/*"
            ]
        }
    ]
}
```

```
    }  
}]
```

Trabalhar com a caixa de diálogo Create Security Group (Criar grupo de segurança)

Você pode criar uma política que permita que os usuários trabalhem com a caixa de diálogo Create Security Group (Criar grupo de segurança) no console do Amazon EC2. Para usar essa caixa de diálogo, os usuários devem receber a permissão para usar pelo menos as seguintes ações de API:

- `ec2:CreateSecurityGroup`: para criar um novo security group.
- `ec2:DescribeVpcs`: para visualizar uma lista de VPCs existentes na lista VPC.

Com essas permissões, os usuários podem criar um novo security group com êxito, mas não podem adicionar nenhuma regra a ele. Para trabalhar com regras na caixa de diálogo Create Security Group, você pode adicionar as seguintes ações de API à sua política:

- `ec2:AuthorizeSecurityGroupIngress`: para adicionar regras de entrada.
- `ec2:AuthorizeSecurityGroupEgress`: para adicionar regras de saída aos security groups da VPC.
- `ec2:RevokeSecurityGroupIngress`: para modificar ou excluir regras de entrada existentes. Isso é útil para permitir que os usuários usem o recurso Copy to new no console. Esse recurso abre a caixa de diálogo Create Security Group e preenche-a com as mesmas regras do security group que foi selecionado.
- `ec2:RevokeSecurityGroupEgress`: para modificar ou excluir regras de saída de security groups da VPC. Isso é útil para permitir que os usuários modifiquem ou excluam a regra de saída padrão que permite todo o tráfego de saída.
- `ec2>DeleteSecurityGroup`: para prover quando regras inválidas não podem ser salvas. O console primeiro cria o security group e, em seguida, adiciona as regras especificadas. Se as regras forem inválidas, a ação falhará, e o console tentará excluir o security group. O usuário permanece na caixa de diálogo Create Security Group para que possa corrigir a regra inválida e tentar criar o security group novamente. Essa ação de API não é necessária, mas se um usuário não receber permissão para usá-la e tentar criar um security group com regras inválidas, o security group será criado sem nenhuma regra, e o usuário deverá adicioná-las posteriormente.
- `ec2:UpdateSecurityGroupRuleDescriptionsIngress`: para adicionar ou atualizar descrições de regras de grupo de segurança de entrada (inbound).
- `ec2:UpdateSecurityGroupRuleDescriptionsEgress`: para adicionar ou atualizar descrições de regras de grupo de segurança de saída (outbound).
- `ec2:ModifySecurityGroupRules`: para modificar as regras do grupo de segurança.
- `ec2:DescribeSecurityGroupRules`: para listar as regras do grupo de segurança.

A política a seguir concede aos usuários permissão para usar a caixa de diálogo Create Security Group e criar regras de entrada e de saída para security groups associados a uma VPC específica (`vpc-1a2b3c4d`). Os usuários podem criar security groups para o EC2-Classic ou outra VPC, mas não podem adicionar nenhuma regra a eles. Da mesma forma, os usuários não podem adicionar nenhuma regra aos security groups existentes não associados à VPC `vpc-1a2b3c4d`. Os usuários também recebem permissão para visualizar todos os security groups no console. Isso facilita aos usuários identificar os security groups aos quais podem adicionar regras de entrada. Essa política também concede permissão aos usuários para excluir security groups associados à VPC `vpc-1a2b3c4d`.

```
{  
    "Version": "2012-10-17",  
    "Statement": [{  
        "Effect": "Allow",  
        "Action": [  
            "ec2:DescribeSecurityGroups",
```

```
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2>DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
    ],
    "Resource": "arn:aws:ec2:region:111122223333:security-group/*",
    "Condition": {
        "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:111122223333:vpc/vpc-1a2b3c4d"
        }
    }
}
]
```

Exemplo: trabalhar com endereços IP elásticos

Para permitir que os usuários visualizem endereços IP elásticos no console do Amazon EC2, você deve conceder aos usuários permissão para usar a ação `ec2:DescribeAddresses`.

Para permitir que os usuários trabalhem com endereços IP elásticos, você pode adicionar as seguintes ações à política.

- `ec2:AllocateAddress`: para alocar um endereço IP elástico.
- `ec2:ReleaseAddress`: para liberar um endereço IP elástico.
- `ec2:AssociateAddress`: para associar um endereço IP elástico a uma instância ou a uma interface de rede.
- `ec2:DescribeNetworkInterfaces` e `ec2:DescribeInstances`: para trabalhar com a tela Associate address. A tela exibe as instâncias disponíveis ou as interfaces de rede para que você possa associar um endereço IP elástico.
- `ec2:DisassociateAddress`: para desassociar um endereço IP elástico de uma instância ou de uma interface de rede.

As políticas a seguir permitem que os usuários visualizem, aloquem e associem endereços IP elásticos a instâncias. Os usuários não podem associar endereços IP elásticos a interfaces de rede, desassociar endereços IP elásticos ou liberá-los.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemplo: trabalhar com Instâncias reservadas

A política a seguir pode ser anexada a um usuário do IAM. Ela dá ao usuário acesso para visualizar e modificar instâncias reservadas em sua conta, bem como para adquirir novas instâncias reservadas no AWS Management Console.

Esta política permite que os usuários visualizem todas as Instâncias reservadas, bem como Instâncias on-demand, na conta. Não é possível definir permissões em nível de recurso para Instâncias reservadas individuais.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeReservedInstances",  
                "ec2:ModifyReservedInstances",  
                "ec2:PurchaseReservedInstancesOffering",  
                "ec2:DescribeInstances",  
                "ec2:DescribeInstanceTypes",  
                "ec2:DescribeAvailabilityZones",  
                "ec2:DescribeReservedInstancesOfferings"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

A ação `ec2:DescribeAvailabilityZones` é necessária para garantir que o console do Amazon EC2 possa exibir informações sobre as zonas de disponibilidade nas quais você pode comprar Instâncias reservadas. A ação `ec2:DescribeInstances` não é necessária, mas garante que o usuário possa visualizar as instâncias na conta e comprar reservas para atender às especificações corretas.

Você pode ajustar as ações de API para limitar o acesso do usuário, por exemplo, a remoção de `ec2:DescribeInstances` e de `ec2:DescribeAvailabilityZones` significa que o usuário tem acesso somente leitura.

Políticas gerenciadas da AWS para o Amazon Elastic Compute Cloud

Para adicionar permissões a usuários, grupos e funções, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. É necessário tempo e experiência para [criar políticas gerenciadas pelo cliente do IAM](#) que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas gerenciadas pela AWS. Essas políticas abrangem casos de uso comuns e estão disponíveis na sua conta da AWS. Para obter mais informações sobre políticas gerenciadas pela AWS, consulte [Políticas gerenciadas pela AWS](#) no Manual do usuário do IAM.

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada pela AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

Além disso, a AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política gerenciada pela AWS denominada `ReadOnlyAccess` fornece acesso somente leitura a todos os serviços e recursos da AWS. Quando um serviço executa um novo recurso,

a AWS adiciona permissões somente leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte [Políticas gerenciadas pela AWS para funções de trabalho](#) no Manual do usuário do IAM.

Política gerenciada pela AWS: AmazonEC2FullAccess

Você pode anexar a política `AmazonEC2FullAccess` a suas identidades do IAM. Essa política concede permissões que possibilitam acesso total ao Amazon EC2.

Para visualizar as permissões para esta política, consulte [AmazonEC2FullAccess](#) no AWS Management Console.

Política gerenciada pela AWS: AmazonEC2ReadOnlyAccess

Você pode anexar a política `AmazonEC2ReadOnlyAccess` a suas identidades do IAM. Esta política concede permissões que oferecem acesso somente leitura ao Amazon EC2.

Para visualizar as permissões para esta política, consulte [AmazonEC2ReadOnlyAccess](#) no AWS Management Console.

Política gerenciada da AWS: AWSEC2FleetServiceRolePolicy

Esta política é anexada à função vinculada ao serviço chamada `AWSServiceRoleForEC2Fleet` para permitir que o EC2 Fleet solicite, inicie, encerre e etiquele instâncias para você. Para obter mais informações, consulte [Função vinculada ao serviço para Frota do EC2](#) (p. 743).

Política gerenciada da AWS: AWSEC2SpotFleetServiceRolePolicy

Esta política é anexada à função vinculada ao serviço chamada `AWSServiceRoleForEC2SpotFleet` para permitir que a frota spot inicie e gerencie instâncias para você. Para obter mais informações, consulte [Função vinculada ao serviço para frota spot](#) (p. 774).

Política gerenciada da AWS: AWSEC2SpotServiceRolePolicy

Esta política é anexada à função vinculada ao serviço chamada `AWSServiceRoleForEC2Spot` para permitir que o Amazon EC2 inicie e gerencie instâncias spot para você. Para obter mais informações, consulte [Função vinculada ao serviço para solicitações de instâncias spot](#) (p. 311).

Funções do IAM para Amazon EC2

As aplicações devem assinar suas solicitações de API com as credenciais da AWS. Portanto, se você for um desenvolvedor de aplicações, precisará de uma estratégia para gerenciar credenciais para suas aplicações que executam em instâncias do EC2. Por exemplo, você pode distribuir de maneira segura suas credenciais da AWS para as instâncias, permitindo que as aplicações nessas instâncias usem suas credenciais para assinar solicitações, enquanto protege suas credenciais de outros usuários. Contudo, é um desafio distribuir credenciais para cada instância de maneira segura, especialmente aquelas que a AWS cria em seu nome, como instâncias Spot ou instâncias em grupos do Auto Scaling. Você também deve poder atualizar as credenciais em cada instância quando alterna suas credenciais da AWS.

Projetamos funções do IAM para que suas aplicações possam fazer solicitações de API de suas instâncias de maneira segura, sem exigir que você gerencie as credenciais de segurança que as aplicações usam. Em vez de criar e distribuir suas credenciais da AWS, você pode delegar permissão para fazer solicitações de API usando funções do IAM da seguinte forma:

1. Crie uma função do IAM.
2. Defina quais contas ou serviços da AWS podem assumir a função.

3. Defina quais ações e recursos de API a aplicação pode usar depois de assumir a função.
4. Especifique a função quando você executar a instância ou anexe a função a uma instância existente.
5. Faça com que a aplicação recupere um conjunto de credenciais temporárias e use-as.

Por exemplo, você pode usar funções do IAM para conceder permissões a aplicações em execução em suas instâncias que precisam usar um bucket no Amazon S3. Você pode especificar permissões para funções do IAM criando uma política em formato JSON. Essas são semelhantes às políticas que você cria para os usuários do IAM. Se você alterar uma função, a alteração será propagada para todas as instâncias.

Você só pode anexar uma função do IAM a uma instância, mas pode anexar a mesma função a muitas instâncias. Para obter mais informações sobre como criar e usar funções do IAM, consulte [Funções](#) no Guia do usuário do IAM.

Você pode aplicar permissões em nível de recurso às políticas do IAM para controlar a capacidade de anexar, substituir ou desanexar funções do IAM de uma instância. Para obter mais informações, consulte [Permissões no nível do recurso com suporte para ações de API do Amazon EC2 \(p. 1141\)](#) e o seguinte exemplo: [Exemplo: trabalhar com funções do IAM \(p. 1179\)](#).

Tópicos

- [Perfis de instância \(p. 1196\)](#)
- [Recuperar credenciais de segurança dos metadados da instância \(p. 1196\)](#)
- [Conceder uma permissão de usuário do IAM para transmitir uma função do IAM para uma instância \(p. 1197\)](#)
- [Trabalhar com funções do IAM \(p. 1198\)](#)

Perfis de instância

O Amazon EC2 usa um perfil de instância como um contêiner para uma função do IAM. Se você criar uma função do IAM usando o console do IAM ou o console criará automaticamente um perfil de instância e dará a ele o mesmo nome da função correspondente. Se você usar o console do Amazon EC2 para executar uma instância com uma função do IAM ou anexar uma função do IAM a uma instância, deve escolher a função com base em uma lista de nomes de perfis de instância.

Se você usar a AWS CLI, a API ou um AWS SDK para criar uma função, você cria a função e o perfil da instância como ações separadas, com nomes potencialmente diferentes. Se você usar a AWS CLI, a API ou o AWS SDK para executar uma instância com uma função do IAM ou para anexar uma função do IAM a uma instância, especifique o nome do perfil da instância.

Um perfil de instância pode conter somente uma função do IAM. Este limite não pode ser aumentado.

Para obter mais informações, consulte [Perfis de instâncias](#) no Guia do usuário do IAM.

Recuperar credenciais de segurança dos metadados da instância

Uma aplicação na instância recupera as credenciais de segurança fornecidas pela função no item `iam/security-credentials/role-name` dos metadados da instância. A aplicação recebe as permissões para as ações e recursos que você definiu para a função por meio das credenciais de segurança associadas à função. Essas credenciais de segurança são temporárias e são alternadas automaticamente. Tornamos novas credenciais disponíveis pelo menos cinco minutos antes da expiração das credenciais antigas.

Warning

Se você usar serviços que usam os metadados da instância com funções do IAM, não exponha suas credenciais quando os serviços criarem chamadas HTTP em seu nome. Os tipos de serviços

que podem expor suas credenciais incluem proxies HTTP, serviços de validação HTML/CSS e processadores XML que são compatíveis com a inclusão XML.

O comando a seguir recupera as credenciais de segurança para uma função do IAM denominada s3access.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET - Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

A seguir está um exemplo de saída.

```
{  
    "Code" : "Success",  
    "LastUpdated" : "2012-04-26T16:39:16Z",  
    "Type" : "AWS-HMAC",  
    "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",  
    "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",  
    "Token" : "token",  
    "Expiration" : "2017-05-17T15:09:54Z"  
}
```

Para comandos de aplicações, AWS CLI e Tools for Windows PowerShell que são executados na instância, não é necessário obter as credenciais de segurança temporárias explicitamente – os AWS SDKs, a AWS CLI e o Tools for Windows PowerShell obtêm automaticamente as credenciais do serviço de metadados da instância do EC2 e as usam. Para fazer uma chamada fora da instância usando credenciais de segurança temporárias (por exemplo, para testar as políticas do IAM), você deve fornecer a chave de acesso, a chave secreta e o token da sessão. Para obter mais informações, consulte [Usar credenciais de segurança temporárias para solicitar acesso aos recursos da AWS](#) no Manual do usuário do IAM.

Para obter mais informações sobre os metadados da instância, consulte [Metadados da instância e dados do usuário \(p. 622\)](#). Para obter informações sobre o endereço IP dos metadados da instância, consulte [Recuperar metadados da instância \(p. 630\)](#).

Conceder uma permissão de usuário do IAM para transmitir uma função do IAM para uma instância

Para permitir que um usuário do IAM inicie uma instância com uma função do IAM ou anexe ou substitua uma função do IAM em uma instância existente, você deve conceder ao usuário permissão para usar as seguintes ações de API.

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

A política do IAM a seguir concede permissão aos usuários para iniciar instâncias com uma função do IAM ou para anexar ou substituir uma função do IAM em uma instância existente usando a AWS CLI.

Note

Essa política concede aos usuários do IAM acesso a todas as suas funções especificando o recurso como * na política. No entanto, considere se os usuários que executam instâncias com suas funções (as existentes ou que serão criadas mais tarde) podem receber permissões de que não precisam ou que não devem ter.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:RunInstances",  
                "ec2:AssociateIamInstanceProfile",  
                "ec2:ReplaceIamInstanceProfileAssociation"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "iam:PassRole",  
            "Resource": "*"  
        }  
    ]  
}
```

Para conceder permissão aos usuários para iniciar instâncias com uma função do IAM ou para anexar ou substituir uma função do IAM para uma instância existente usando o console do Amazon EC2, você deve conceder-lhes permissão para usar `iam>ListInstanceProfiles`, `iam:PassRole`, `ec2:AssociateIamInstanceProfile` e `ec2:ReplaceIamInstanceProfileAssociation`, além de quaisquer outras permissões necessárias. Para obter exemplos de políticas do , consulte [Políticas de exemplo para trabalhar no console do Amazon EC2 \(p. 1185\)](#).

Trabalhar com funções do IAM

Você pode criar uma função do IAM e anexá-la a uma instância durante ou depois da execução. Você também pode substituir ou desanexar uma função do IAM para uma instância.

Tópicos

- [Criar uma função do IAM \(p. 1198\)](#)
- [Executar uma instância com uma função do IAM \(p. 1200\)](#)
- [Anexar uma função do IAM a uma instância \(p. 1202\)](#)
- [Substituir uma função do IAM \(p. 1203\)](#)
- [Desanexar uma função do IAM \(p. 1204\)](#)
- [Gerar uma política para sua função do IAM com base na atividade de acesso \(p. 1205\)](#)

Criar uma função do IAM

Você deve criar uma função do IAM para poder executar uma instância com essa função ou anexá-la a uma instância.

Para criar uma função do IAM usando o console do IAM

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.

2. No painel de navegação, escolha Roles e depois Create Role.
3. Na página Select role type, escolha EC2 e o caso de uso EC2. Escolha Próximo: Permissões.
4. Na página Attach permissions policy, selecione uma política gerenciada pela AWS que conceda às suas instâncias acesso aos recursos de que precisam.
5. Na página Review (Revisão), insira um nome para a função e selecione Create role (Criar função).

Como alternativa, você pode usar a AWS CLI para criar uma função do IAM. O exemplo a seguir cria uma função do IAM com uma política que permite que a função use um bucket do Amazon S3.

Para criar uma função do IAM e um perfil de instância (AWS CLI)

1. Crie a seguinte política de confiança e salve-a em um arquivo de texto chamado `ec2-role-trust-policy.json`.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": { "Service": "ec2.amazonaws.com"},  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

2. Crie a função `s3access` e especifique a política de confiança que você criou usando o comando `create-role`.

```
aws iam create-role --role-name s3access --assume-role-policy-document file://ec2-role-trust-policy.json  
{  
    "Role": {  
        "AssumeRolePolicyDocument": {  
            "Version": "2012-10-17",  
            "Statement": [  
                {  
                    "Action": "sts:AssumeRole",  
                    "Effect": "Allow",  
                    "Principal": {  
                        "Service": "ec2.amazonaws.com"  
                    }  
                }  
            ]  
        },  
        "RoleId": "AROAIIZKPBKS2LEXAMPLE",  
        "CreateDate": "2013-12-12T23:46:37.247Z",  
        "RoleName": "s3access",  
        "Path": "/",  
        "Arn": "arn:aws:iam::123456789012:role/s3access"  
    }  
}
```

3. Crie uma política de acesso e salve-a em um arquivo de texto chamado `ec2-role-access-policy.json`. Por exemplo, essa política concede permissões administrativas para o Amazon S3 a aplicações que executam na instância.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {
```

```
        "Effect": "Allow",
        "Action": ["s3:*"],
        "Resource": ["*"]
    }
]
}
```

4. Anexe a política de acesso à função usando o comando [put-role-policy](#).

```
aws iam put-role-policy --role-name s3access --policy-name S3-Permissions --policy-document file:/ec2-role-access-policy.json
```

5. Crie um perfil de instância chamado s3access-profile usando o comando [create-instance-profile](#).

```
aws iam create-instance-profile --instance-profile-name s3access-profile
{
    "InstanceProfile": {
        "InstanceProfileId": "AIPAJTLBPJLEGREXAMPLE",
        "Roles": [],
        "CreateDate": "2013-12-12T23:53:34.093Z",
        "InstanceProfileName": "s3access-profile",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:instance-profile/s3access-profile"
    }
}
```

6. Adicione a função s3access ao perfil de instância s3access-profile.

```
aws iam add-role-to-instance-profile --instance-profile-name s3access-profile --role-name s3access
```

Como alternativa, você pode usar os seguintes comandos do AWS Tools for Windows PowerShell:

- [New-IAMRole](#)
- [Register-IAMRolePolicy](#)
- [New-IMAMInstanceProfile](#)

Executar uma instância com uma função do IAM

Depois de criar uma função do IAM, você pode executar uma instância e associar essa função à instância durante a execução.

Important

Depois de criar uma função do IAM, pode demorar vários segundos para as permissões serem propagadas. Se sua primeira tentativa de executar uma instância com uma função falhar, aguarde alguns segundos antes de tentar novamente. Para obter mais informações, consulte [Como solucionar problemas ao trabalhar com funções](#) no Guia do usuário do IAM.

Para executar uma instância com uma função do IAM (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel, escolha Executar instância.
3. Selecione um AMI e um tipo de instância e escolha Next: Configure Instance Details.
4. Na página Configure Instance Details, para IAM role, selecione a função do IAM que você criou.

Note

A lista IAM role exibe o nome do perfil da instância que você criou ao criar a função do IAM. Se você tiver criado a função do IAM usando o console, o perfil da instância terá sido criado para você e recebido o mesmo nome da função. Se tiver criado a função do IAM usando a AWS CLI, a API ou um AWS SDK, você poderá ter dado um nome diferente para o perfil da instância.

5. Configure todos os outros detalhes e siga as instruções no restante do assistente, ou escolha Review and Launch para aceitar as configurações padrão e vá diretamente para a página Review Instance Launch.
6. Reveja as configurações e selecione Launch para escolher um par de chaves e executar a instância.
7. Se você estiver usando as ações da API do Amazon EC2 em sua aplicação, recupere as credenciais de segurança da AWS disponibilizadas na instância e use-as para assinar as solicitações. O AWS SDK da cuida disso para você.

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Como alternativa, você pode usar a AWS CLI para associar uma função a uma instância durante a execução. Você deve especificar o perfil da instância no comando.

Para executar uma instância com uma função do IAM (AWS CLI)

1. Use o comando [run-instances](#) para executar uma instância usando o perfil da instância. O exemplo a seguir mostra como executar uma instância com o perfil da instância.

```
AWS ec2 run-instances \
--image-id ami-11aa22bb \
--iam-instance-profile Name="s3access-profile" \
--key-name my-key-pair \
--security-groups my-security-group \
--subnet-id subnet-1a2b3c4d
```

Como alternativa, use o comando [New-EC2Instance](#) do Tools for Windows PowerShell.

2. Se você estiver usando as ações da API do Amazon EC2 em sua aplicação, recupere as credenciais de segurança da AWS disponibilizadas na instância e use-as para assinar as solicitações. O AWS SDK da cuida disso para você.

```
curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Anexar uma função do IAM a uma instância

Para anexar uma função do IAM a uma instância sem função, a instância pode estar no estado `stopped` ou `running`.

New console

Como anexar uma função do IAM a uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Security (Segurança), Modify IAM role (Modificar função do IAM).
4. Selecione a função do IAM a ser anexada à instância e selecione Save (Salvar).

Old console

Como anexar uma função do IAM a uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions, Instance Settings, Attach/Replace IAM role.
4. Selecione a função do IAM a ser anexada à instância e escolha Apply (Aplicar).

Para anexar uma função do IAM a uma instância (AWS CLI)

1. Se necessário, descreva as instâncias para obter o ID da instância à qual anexar a função.

```
aws ec2 describe-instances
```

2. Use o comando `associate-iam-instance-profile` para anexar a função do IAM à instância especificando o perfil de instância. Você pode usar o Nome de recursos da Amazon (ARN) do perfil da instância ou seu nome.

```
aws ec2 associate-iam-instance-profile \
--instance-id i-1234567890abcdef0 \
--iam-instance-profile Name="TestRole-1"

{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-1234567890abcdef0",
        "State": "associating",
        "AssociationId": "iip-assoc-0dbd8529a48294120",
        "IamInstanceProfile": {
            "Id": "AIPAJLNLDX3AMYZNWYYAY",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-1"
        }
    }
}
```

Como alternativa, use os seguintes comandos do Tools for Windows PowerShell:

- `Get-EC2Instance`
- `Register-EC2IamInstanceProfile`

Substituir uma função do IAM

Para substituir a função do IAM em uma instância que já tenha uma função do IAM anexa, a instância deve estar no estado `running`. Você poderá fazer isso se quiser alterar a função do IAM de uma instância sem desanexar a existente primeiro. Por exemplo, você pode fazer isso para garantir que as ações de API desempenhadas por aplicações executadas na instância não sejam interrompidas.

New console

Como substituir uma função do IAM para uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Security (Segurança), Modify IAM role (Modificar função do IAM).
4. Selecione a função do IAM a ser anexada à instância e selecione Save (Salvar).

Old console

Como substituir uma função do IAM para uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions, Instance Settings, Attach/Replace IAM role.
4. Selecione a função do IAM a ser anexada à instância e escolha Apply (Aplicar).

Para substituir uma função do IAM em uma instância (AWS CLI)

1. Se necessário, descreva as associações do perfil da instância do IAM para obter o ID da associação do perfil da instância do IAM a ser substituído.

```
aws ec2 describe-iam-instance-profile-associations
```

2. Use o comando `replace-iam-instance-profile-association` para substituir o perfil de instância do IAM especificando o ID da associação do perfil da instância existente e o ARN ou o nome do perfil da instância que deve substituí-lo.

```
aws ec2 replace-iam-instance-profile-association \
--association-id iip-assoc-0044d817db6c0a4ba \
--iam-instance-profile Name="TestRole-2"  
  
{  
    "IamInstanceProfileAssociation": {  
        "InstanceId": "i-087711ddaf98f9489",  
        "State": "associating",  
        "AssociationId": "iip-assoc-09654be48e33b91e0",  
        "IamInstanceProfile": {  
            "Id": "AIPAJCJEDKX7QYHWYK7GS",  
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"  
        }  
    }  
}
```

Como alternativa, use os seguintes comandos do Tools para Windows PowerShell:

- [Get-EC2IamInstanceProfileAssociation](#)
- [Set-EC2IamInstanceProfileAssociation](#)

Desanexar uma função do IAM

Você pode desanexar uma função do IAM de uma instância em execução ou parada.

New console

Como desanexar uma função do IAM de uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions (Ações), Security (Segurança), Modify IAM role (Modificar função do IAM).
4. Em IAM role (Função do IAM), selecione No IAM Role (Nenhuma função do IAM). Escolha Save (Salvar).
5. Na caixa de diálogo de confirmação, insira Detach (Desanexar) e selecione Detach (Desanexar).

Old console

Como desanexar uma função do IAM de uma instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância, escolha Actions, Instance Settings, Attach/Replace IAM role.
4. Em IAM role, escolha No Role. Escolha Aplicar.
5. Na caixa de diálogo de confirmação, escolha Sim, separar.

Para desanexar uma função do IAM de uma instância (AWS CLI)

1. Se necessário, use [describe-iam-instance-profile-associations](#) para descrever as associações do perfil da instância do IAM e obter o ID da associação do perfil da instância do IAM a ser desanexado.

```
aws ec2 describe-iam-instance-profile-associations

{
    "IamInstanceProfileAssociations": [
        {
            "InstanceId": "i-088ce778fbfeb4361",
            "State": "associated",
            "AssociationId": "iip-assoc-0044d817db6c0a4ba",
            "IamInstanceProfile": {
                "Id": "AIPAJEDNCAA64SSD265D6",
                "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
            }
        }
    ]
}
```

2. Use o comando [disassociate-iam-instance-profile](#) para desanexar o perfil da instância do IAM usando o ID da associação.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-assoc-0044d817db6c0a4ba
```

```
{  
    "IamInstanceProfileAssociation": {  
        "InstanceId": "i-087711ddaf98f9489",  
        "State": "disassociating",  
        "AssociationId": "iip-assoc-0044d817db6c0a4ba",  
        "IamInstanceProfile": {  
            "Id": "AIPAJEDNCAA64SSD265D6",  
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"  
        }  
    }  
}
```

Como alternativa, use os seguintes comandos do Tools para Windows PowerShell:

- [Get-EC2IamInstanceProfileAssociation](#)
- [Unregister-EC2IamInstanceProfile](#)

Gerar uma política para sua função do IAM com base na atividade de acesso

Quando você cria uma função do IAM pela primeira vez para suas aplicações, às vezes você pode conceder permissões além do que é necessário. Antes de iniciar sua aplicação em seu ambiente de produção, você pode gerar uma política do IAM baseada na atividade de acesso para uma função do IAM. O IAM Access Analyzer revisa seus logs do AWS CloudTrail registra e gera um modelo de política que contém as permissões que foram usadas pela função no intervalo de datas especificado. Você pode usar o modelo para criar uma política gerenciada com permissões refinadas e anexá-la à função do IAM. Dessa forma, você concede apenas as permissões necessárias à interação com os recursos da AWS, de acordo com a especificidade do caso de uso. Isso ajuda você a aderir às melhores práticas de [conceder privilégio mínimo](#). Para saber mais, consulte [Gerar políticas com base na atividade de acesso](#) no Guia do usuário do IAM.

Autorizar tráfego de entrada para suas instâncias do Windows

Os security groups permitem controlar o tráfego para sua instância incluindo o tipo de tráfego que pode acessar sua instância. Por exemplo, você pode permitir que apenas os computadores de sua rede local acessem sua instância usando RDP. Se sua instância for um servidor Web, você poderá permitir que todos os endereços IP acessem sua instância usando HTTP ou HTTPS, para que os usuários externos possam navegar pelo conteúdo de seu servidor Web.

Os grupos de segurança padrão e os grupos de segurança recém-criados incluem regras padrão que não permitem que você acesse a instância pela internet. Para obter mais informações, consulte [Grupos de segurança padrão \(p. 1222\)](#) e [Os security groups personalizados \(p. 1223\)](#). Para permitir acesso da rede para sua instância, você deverá permitir o tráfego de entrada para sua instância. Para abrir uma porta para o tráfego de entrada, adicione uma regra a um security group que você associou à instância quando a executou.

Para conectar-se à instância, você deve configurar uma regra para autorizar tráfego do RDP no endereço IPv4 público de seu computador. Para permitir tráfego do RDP de intervalos de endereços IP adicionais, adicione outra regra para cada intervalo que você precisar autorizar.

Se você tiver habilitado sua VPC para IPv6 e executou a instância com um endereço IPv6, você poderá conectar-se à instância usando seu endereço IPv6 em vez de um endereço IPv4 público. Seu computador local deve ter um endereço IPv6 e configurado para usar IPv6.

Se você precisar permitir acesso de rede a uma instância Linux, consulte [Como autorizar tráfego de entrada para suas instâncias Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Antes de começar

Decida quem requer acesso à instância. Por exemplo, um único host ou uma rede específica em que você confia, como o endereço IPv4 público de seu computador local. O editor do security group no console do Amazon EC2 pode detectar automaticamente o endereço IPv4 público de seu computador local. Como alternativa, você pode usar a frase de pesquisa "qual é meu endereço IP" em um navegador de Internet ou o serviço a seguir: [Verificar IP](#). Se estiver conectado por meio de um ISP ou atrás de um firewall sem um endereço IP estático, localize o intervalo de endereços IP usado por computadores cliente.

Warning

Se usar `0.0.0.0/0`, permitirá que todos os endereços IPv4 acessem sua instância usando RDP. Se usar `:/:0`, você permitirá que todos os endereços IPv6 acessem sua instância. Isso é aceitável para um período curto em um ambiente de teste, mas não é seguro em ambientes de produção. Na produção, você autorizará somente um endereço IP específico ou intervalo de endereços para acessar a instância.

O Firewall do Windows também pode bloquear o tráfego de entrada. Se estiver tendo problemas para configurar o acesso à instância, você poderá precisar desabilitar o Firewall do Windows. Para obter mais informações, consulte [O Remote Desktop não pode se conectar ao computador remoto \(p. 1574\)](#).

Adicionar uma regra para o tráfego de entrada do RDP a uma instância do Windows

Os security groups atuam como firewall para instâncias associadas, controlando o tráfego de entrada e de saída no nível da instância. Você deve adicionar regras a um grupo de segurança que permitam que você se conecte à instância do Windows no seu endereço IP usando o RDP.

New console

Para adicionar uma regra a um grupo de segurança para tráfego de entrada do RDP por meio de IPv4 (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione sua instância e, na metade inferior da tela, escolha a guia Security (Segurança) . O parâmetro Security groups (Grupos de segurança) lista os grupos de segurança associados à instância. O parâmetro Inbound rules (Regras de entrada) exibem uma lista das regras de entrada que estão em vigor para a instância.
4. Para o grupo de segurança ao qual você adicionará a nova regra, escolha o link ID do grupo de segurança para abrir o grupo de segurança.
5. Na guia Inbound Rules (Regras de entrada), selecione Edit inbound rules (Editar regras de entrada).
6. Na página Edit inbound rules (Editar regras de entrada) , faça o seguinte:
 - a. Escolha Add rule (Adicionar regra).
 - b. Em Type, escolha RDP.
 - c. Na caixa Source (Fonte), escolha My IP (Meu IP) para preencher automaticamente o campo com o endereço IPv4 público do computador local.

Como alternativa, para Source (Fonte), escolha Custom (Personalizado) e insira o endereço IPv4 público do computador ou da rede em notação CIDR. Por exemplo, se o endereço IPv4 for `203.0.113.25`, insira `203.0.113.25/32` para listar esse único endereço IPv4 em notação CIDR. Se sua empresa alocar endereços com base em um intervalo, insira o intervalo inteiro, como `203.0.113.0/24`.

Para obter informações sobre como localizar seu endereço IP, consulte [Antes de começar \(p. 1206\)](#).

- d. Selecione Save rules (Salvar regras).

Old console

Para adicionar uma regra a um grupo de segurança para tráfego de entrada do RDP por meio de IPv4 (console)

1. No painel de navegação do console do Amazon EC2, escolha Instances (Instâncias). Selecione a instância e procure a guia Description. A opção Security groups lista os security groups associados à instância. Escolha view inbound rules (visualizar regras de entrada) para exibir uma lista das regras que estão em vigor na instância.
2. No painel de navegação, selecione Grupos de segurança. Selecione um dos security groups associados à instância.
3. No painel de detalhes, na guia Inbound, escolha Edit. Na caixa de diálogo, escolha Add Rule (Adicionar regra) e, em seguida, escolha RDP na lista Type (Tipo).
4. No campo Source, escolha My IP para preencher automaticamente o campo com o endereço IPv4 público do computador local. Como alternativa, escolha Custom e especifique o endereço IPv4 público do computador ou da rede em notação CIDR. Por exemplo, se o endereço IPv4 for 203.0.113.25, especifique 203.0.113.25/32 para listar esse único endereço IPv4 em notação CIDR. Se sua empresa alocar endereços de um intervalo, especifique o intervalo inteiro, como 203.0.113.0/24.

Para obter informações sobre como localizar seu endereço IP, consulte [Antes de começar \(p. 1206\)](#).

5. Escolha Save (Salvar).

Se você executou uma instância com um endereço IPv6 e desejar conectar-se à sua instância usando seu endereço IPv6, você deverá adicionar regras que permitam o tráfego IPv6 de entrada via RDP.

New console

Para adicionar uma regra a um grupo de segurança para tráfego de entrada do RDP por meio de IPv6 (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione sua instância e, na metade inferior da tela, escolha a guia Security (Segurança) . O parâmetro Security groups (Grupos de segurança) lista os grupos de segurança associados à instância. O parâmetro Inbound rules (Regras de entrada) exibem uma lista das regras de entrada que estão em vigor para a instância.
4. Para o grupo de segurança ao qual você adicionará a nova regra, escolha o link ID do grupo de segurança para abrir o grupo de segurança.
5. Na guia Inbound Rules (Regras de entrada), selecione Edit inbound rules (Editar regras de entrada).
6. Na página Edit inbound rules (Editar regras de entrada) , faça o seguinte:
 - a. Escolha Add rule (Adicionar regra).
 - b. Em Type, escolha RDP.
 - c. Em Source (Origem), escolha Custom (Personalizado) e insira o endereço IPv6 do computador em notação CIDR. Por exemplo, se seu endereço

IPv6 for 2001:db8:1234:1a00:9691:9503:25ad:1761, insira 2001:db8:1234:1a00:9691:9503:25ad:1761/128 para listar este único endereço IP em notação CIDR. Se sua empresa alocar endereços com base em um intervalo, insira o intervalo inteiro, como 2001:db8:1234:1a00::/64.

- d. Selecione Save rules (Salvar regras).

Old console

Para adicionar uma regra a um grupo de segurança para tráfego de entrada do RDP por meio de IPv6 (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança. Selecione o security group de sua instância.
3. Escolha Inbound, Edit, Add Rule.
4. Em Type, escolha RDP.
5. No campo Source, especifique o endereço IPv6 de seu computador em notação CIDR. Por exemplo, se seu endereço IPv6 for 2001:db8:1234:1a00:9691:9503:25ad:1761, especifique 2001:db8:1234:1a00:9691:9503:25ad:1761/128 para listar esse único endereço IP em notação CIDR. Se sua empresa alocar endereços de um intervalo, especifique o intervalo inteiro, como 2001:db8:1234:1a00::/64.
6. Escolha Save (Salvar).

Note

Execute os comandos a seguir no sistema local, não na própria instância. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

Para adicionar uma regra a um security group usando a linha de comando

1. Encontre o security group que está associado à sua instância usando um dos seguintes comandos:

- [describe-instance-attribute](#) (AWS CLI)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute groupSet
```

- [Get-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId instance_id -Attribute groupSet).Groups
```

Os dois comandos retornam um ID de security group que será usado na próxima etapa.

2. Adicione a regra ao security group usando um dos seguintes comandos:

- [authorize-security-group-ingress](#) (AWS CLI)

```
aws ec2 authorize-security-group-ingress --group-id security_group_id --protocol tcp --port 3389 --cidr cidr_ip_range
```

- [Grant-EC2SecurityGroupIngress](#) (AWS Tools for Windows PowerShell)

O comando `Grant-EC2SecurityGroupIngress` precisa de um parâmetro `IpPermission` que descreve o protocolo, o intervalo de portas e o intervalo de endereços IP a serem usados para a regra de security group. O comando a seguir cria o parâmetro `IpPermission`:

```
PS C:\> $ip1 = @{ IpProtocol="tcp"; FromPort="3389"; ToPort="3389";  
IpRanges="cidr_ip_range" }
```

```
PS C:\> Grant-EC2SecurityGroupIngress -GroupId security_group_id -IpPermission  
@($ip1)
```

Atribuir um grupo de segurança a uma instância

Você pode atribuir um security group a uma instância ao executá-la. Quando você adiciona ou remove regras, essas alterações são aplicadas automaticamente a todas as instâncias às quais você atribuiu o security group.

Depois de executar uma instância, você pode alterar seus security groups. Para obter mais informações, consulte [Alterar os grupos de segurança de uma instância](#) no Guia do usuário da Amazon VPC.

Pares de chaves do Amazon EC2 e instâncias do Windows

Um par de chaves, que consiste em uma chave pública e uma chave privada, trata-se de um conjunto de credenciais de segurança usadas para provar sua identidade ao se conectar a uma instância do Amazon EC2. O Amazon EC2 armazena a chave pública na instância, e você armazena a chave privada. Para instâncias do Windows, é necessária uma chave privada para descriptografar a senha de administrador. Use a senha descriptografada para se conectar à instância. Qualquer pessoa que tenha a sua chave privada pode se conectar a suas instâncias. Por isso é importante que você armazene a chave privada em um lugar seguro.

Ao executar uma instância, um [par de chaves será solicitado \(p. 425\)](#). Se você planeja se conectar à instância usando RDP, deverá especificar um par de chaves. É possível escolher um par de chaves existente ou criar um novo. Com instâncias do Windows, use a chave privada para obter a senha de administrador e faça login usando RDP. Para obter mais informações sobre como se conectar à sua instância, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#). Para obter mais informações sobre pares de chaves e instâncias do Linux, consulte [Pares de chaves do Amazon EC2 e instâncias do Linux](#) no Manual do usuário do Amazon EC2 para instâncias do Linux.

Como o Amazon EC2 não mantém uma cópia da sua chave privada, não há como recuperar a chave privada caso você a perca. No entanto, ainda pode haver uma maneira de se conectar a instâncias para as quais você perdeu a chave privada. Para obter mais informações, consulte [Conectar-se à instância do Windows se você perder a chave privada \(p. 1217\)](#).

Você pode usar o Amazon EC2 para criar pares de chaves. Também é possível usar uma ferramenta de terceiros para criar pares de chaves e importar as chaves públicas para o Amazon EC2.

As chaves que o Amazon EC2 usa são chaves SSH-2 RSA ED25519 ou de 2048 bit.

É possível ter até 5.000 pares de chaves por região.

Tópicos

- [Criar um par de chaves usando o Amazon EC2 \(p. 1210\)](#)
- [Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2 \(p. 1211\)](#)
- [Etiquetar uma chave pública \(p. 1213\)](#)
- [Recuperar a chave pública da chave privada \(p. 1214\)](#)

- Recuperar a chave pública por meio de metadados de instância (p. 1215)
- Identificar o par de chaves que foi especificado na execução (p. 1215)
- Verificar a impressão digital do par de chaves (p. 1215)
- Excluir o par de chaves (p. 1216)
- Conectar-se à instância do Windows se você perder a chave privada (p. 1217)

Criar um par de chaves usando o Amazon EC2

Você pode criar um par de chaves usando um dos seguintes métodos.

Console

Como criar o par de chaves

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em Rede e segurança, selecione Pares de chaves.
3. Escolha Create key pair (Criar par de chaves).
4. Em Name (Nome), insira um nome descritivo para o par de chaves. O Amazon EC2 associa a chave pública ao nome especificado como o nome da chave. Um nome de chave pode incluir até 255 caracteres ASCII. Não pode incluir espaços no início nem no final.
5. Para o tipo de par de chaves, escolha RSA ou ED25519. Note que as chaves ED25519 não são compatíveis com instâncias do Windows, EC2 Instance Connect ou Console de série do EC2.
6. Para Formato de arquivo de chave privada, escolha o formato no qual salvar a chave privada. Para salvar a chave privada em um formato que possa ser usado com o OpenSSH, escolha pem. Para salvar a chave privada em um formato que possa ser usado com o PUTTY, escolha ppk.

Se você escolheu ED25519 na etapa anterior, o formato de arquivo de chaves privadas não aparece, e o formato de chave privada é o padrão PEM.

7. Para adicionar uma etiqueta à chave pública, escolha Adicionar etiqueta, e insira a chave e o valor da etiqueta. Repita esse procedimento para cada tag.
8. Escolha Create key pair (Criar par de chaves).
9. O arquivo de chave privada é baixado automaticamente pelo navegador. O nome do arquivo base é o nome especificado como o nome do par de chaves, e a extensão do nome do arquivo é determinada pelo formato do arquivo escolhido. Salve o arquivo de chave privada em um lugar seguro.

Important

Esta é a única chance de você salvar o arquivo de chave privada.

AWS CLI

Como criar o par de chaves

- Use o comando `create-key-pair` da seguinte forma para gerar um par de chaves e salvar a chave privada em um arquivo .pem.

Para o `--key-name`, especifique um nome para a chave pública. O nome pode incluir até 255 caracteres ASCII.

Para o `--key-type`, especifique `rsa` ou `ed25519`. Se você não incluir o parâmetro `--key-type`, qualquer chave `rsa` é criada por padrão. Observe que as chaves ED25519 não são compatíveis com instâncias do Windows, EC2 Instance Connect e Console de série do EC2.

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Criar um par de chaves usando uma ferramenta de
terceiros e importe a chave pública para o Amazon EC2

--query "KeyMaterial" imprime o material da chave privada para a saída.

--output text > *my-key-pair*.pem salva o material da chave privada em um arquivo com a extensão .pem. A chave privada pode ter um nome diferente do nome da chave pública mas, para facilitar o uso, use o mesmo nome.

```
aws ec2 create-key-pair \
--key-name my-key-pair \
--key-type rsa \
--query "KeyMaterial" \
--output text > my-key-pair.pem
```

PowerShell

Como criar o par de chaves

Use o comando do AWS Tools for Windows PowerShell, [New-EC2KeyPair](#), da seguinte forma para gerar a chave e salvá-la em um arquivo .pem.

Para o **-KeyName**, especifique um nome para a chave pública. O nome pode incluir até 255 caracteres ASCII.

Para o **-KeyType**, especifique **rsa** ou **ed25519**. Se você não incluir o parâmetro **-KeyType**, qualquer chave **rsa** é criada por padrão. Observe que as chaves ED25519 não são compatíveis com instâncias do Windows, EC2 Instance Connect e Console de série do EC2.

KeyMaterial imprime o material da chave privada para a saída.

Out-File -Encoding ascii -FilePath *C:\path\my-key-pair*.pem salva o material da chave privada em um arquivo com a extensão .pem. A chave privada pode ter um nome diferente do nome da chave pública mas, para facilitar o uso, use o mesmo nome.

```
PS C:\> (New-EC2KeyPair -KeyName "my-key-pair" -KeyType "rsa").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2

Em vez de usar o Amazon EC2 para criar seu par de chaves, você pode criar um par de chaves de RSA ou ED25519 usando uma ferramenta de terceiros e, então, importar a chave pública para o Amazon EC2.

Requisitos para pares de chaves

- Tipos compatíveis: RSA e ED25519. O Amazon EC2 não aceita chaves DSA.
- Observe que as chaves ED25519 não são compatíveis com instâncias do Windows, EC2 Instance Connect e Console de série do EC2.
- Formatos com suporte
 - Formato de chave pública de OpenSSH
 - O formato de arquivo de chave privada SSH deve ser PEM
 - (Apenas RSA) Formato DER codificado em Base64
 - (Apenas RSA) Formato de arquivo de chave pública SSH, conforme especificado em [RFC 4716](#)

- Tamanhos compatíveis: 1024, 2048 e 4096.

Para criar um par de chaves usando uma ferramenta de terceiros

1. Gere um par de chaves com uma ferramenta de terceiros de sua escolha. Por exemplo, você pode usar ssh-keygen (uma ferramenta fornecida com a instalação padrão de OpenSSH). Como alternativa, Java, Ruby, Python e muitas outras linguagens de programação fornecem bibliotecas padrão que você pode usar para criar um par de chaves de RSA ou ED25519.

Important

A chave privada deve estar no formato PEM. Por exemplo, use `ssh-keygen -m PEM` para gerar a chave OpenSSH no formato PEM.

2. Salve a chave pública em um arquivo local. Por exemplo, `C:\keys\my-key-pair.pub`. A extensão do nome de arquivo para esse arquivo não é importante.
3. Salve a chave privada em um arquivo local que tenha a extensão `.pem`. Por exemplo, `C:\keys\my-key-pair.pem`. A extensão do nome deste arquivo é importante porque somente os arquivos `.pem` podem ser selecionados quando for feita a conexão à instância do Windows a partir do console do EC.

Important

Salve o arquivo de chave privada em um lugar seguro. Você precisará fornecer o nome da chave pública ao iniciar uma instância e a chave privada correspondente sempre que se conectar à instância.

Depois de criar o par de chaves, use um dos seguintes métodos para importar o par de chaves para Amazon EC2.

Console

Para importar a chave pública

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Key Pairs (Pares de chaves).
3. Selecione Import key pair (Importar par de chaves).
4. Em Name (Nome), insira um nome descritivo para a chave pública. O nome pode incluir até 255 caracteres ASCII. Não pode incluir espaços no início nem no final.

Note

Quando você se conecta à instância pelo console do EC2, o console sugere esse nome para o arquivo de chave privada.

5. Escolha Browse (Procurar) para navegar e selecionar a chave pública ou cole o conteúdo da chave pública no campo Public key contents (Conteúdo da chave pública).
6. Selecione Import key pair (Importar par de chaves).
7. Verifique se a chave pública que você importou aparece na lista de pares de chaves.

AWS CLI

Para importar a chave pública

Use o comando `import-key-pair` da AWS CLI.

Como verificar se o par de chaves foi importado com êxito

Use o comando `describe-key-pairs` da AWS CLI.

PowerShell

Para importar a chave pública

Use o comando [Import-EC2KeyPair](#) do AWS Tools for Windows PowerShell.

Como verificar se o par de chaves foi importado com êxito

Use o comando [Get-EC2KeyPair](#) do AWS Tools for Windows PowerShell.

Etiquetar uma chave pública

Para categorizar e gerenciar as chaves públicas que você criou usando o Amazon EC2 ou importou para o Amazon EC2, é possível etiquetá-las com metadados personalizados. Para obter mais informações sobre como as tags funcionam, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

Você pode visualizar, adicionar e excluir etiquetas usando um dos seguintes métodos.

Console

Como exibir, adicionar ou excluir uma tag para uma chave pública existente

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Key Pairs (Pares de chaves).
3. Selecione uma chave pública e escolha Actions (Ações), Manage tags (Gerenciar etiquetas).
4. A página Manage tags (Gerenciar etiquetas) exibe todas as etiquetas atribuídas à chave pública.
 - Para adicionar uma tag, escolha Add tag (Adicionar tag), e insira a chave e o valor da tag. Você pode adicionar até 50 etiquetas por chave. Para obter mais informações, consulte [Restrições de tags \(p. 1558\)](#).
 - Para excluir uma tag, escolha Remove (Remover) ao lado da tag que será excluída.
5. Escolha Save (Salvar).

AWS CLI

Para exibir etiquetas de chave pública

Use o comando [describe-tags](#) da AWS CLI. No exemplo a seguir, descreva as etiquetas para todos as suas chaves o públicas.

```
C:\> aws ec2 describe-tags --filters "Name=resource-type,Values=key-pair"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "key-0123456789EXAMPLE",
            "ResourceType": "key-pair",
            "Value": "Production"
        },
        {
            "Key": "Environment",
            "ResourceId": "key-9876543210EXAMPLE",
            "ResourceType": "key-pair",
            "Value": "Production"
        }
    ]
}
```

```
}
```

Como descrever as etiquetas de uma chave pública específica

Use o comando [describe-key-pairs](#) da AWS CLI.

```
C:\> aws ec2 describe-key-pairs --key-pair-ids key-0123456789EXAMPLE
```

```
{
    "KeyPairs": [
        {
            "KeyName": "MyKeyPair",
            "KeyFingerprint": "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyId": "key-0123456789EXAMPLE",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                }
            ]
        }
    ]
}
```

Para etiquetar uma chave pública existente

Use o comando da AWS CLI [create-tags](#). No exemplo a seguir, o par de chaves existente está marcado com Key=Cost-Center e Value=CC-123.

```
C:\> aws ec2 create-tags --resources key-0123456789EXAMPLE --tags Key=Cost-Center,Value=CC-123
```

Como excluir uma etiqueta de uma chave pública

Use o comando [delete-tags](#) da AWS CLI. Para obter exemplos, consulte [Examples \(Exemplos\)](#) na AWS CLI Command Reference (Referência de comandos da AWS CLI).

PowerShell

Para exibir etiquetas de chave pública

Use o comando [Get-EC2Tag](#).

Como descrever as etiquetas de uma chave pública específica

Use o comando [Get-EC2KeyValuePair](#).

Para etiquetar uma chave pública existente

Use o comando [New-EC2Tag](#).

Como excluir uma etiqueta de uma chave pública

Use o comando [Remove-EC2Tag](#).

Recuperar a chave pública da chave privada

Em seu computador Windows local, você pode usar o PuTTYgen para obter a chave pública do seu par de chaves.

Inicie o PuTTYgen e selecione Load (Carregar). Selecione o arquivo .ppk ou .pem de chave privada. O PuTTYgen exibe a chave pública em Public key for pasting into OpenSSH authorized_keys file (Chave pública para colar no arquivo authorized_keys do OpenSSH). Também é possível visualizar a chave pública selecionando Save public key (Salvar a chave pública), especificando um nome para o arquivo, salvando-o e abrindo-o.

Recuperar a chave pública por meio de metadados de instância

A chave pública que você especificou ao executar uma instância também está disponível por meio dos metadados da instância. Para ver a chave pública especificada ao iniciar a instância, use o comando a seguir a partir da sua instância.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Veja a seguir um exemplo de saída.

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706Vhz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXrlsLnBItntckij7FbtJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzzqaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkyQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3RbBQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYWI3f05p6KLxEXAMPLE my-key-pair
```

Se você alterar o par de chaves usado para conectar-se à instância, não atualizaremos os metadados da instância para mostrar a nova chave pública. Em vez disso, os metadados da instância continuam a mostrar a chave pública do par de chaves especificado quando você executou a instância. Para obter mais informações, consulte [Recuperar metadados da instância \(p. 630\)](#).

Identificar o par de chaves que foi especificado na execução

Ao executar uma instância, um [par de chaves será solicitado \(p. 425\)](#). Se você planeja se conectar à instância usando RDP, deverá especificar um par de chaves.

Como identificar o par de chaves que foi especificado na execução

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias e, em seguida, sua instância.
3. Na guia Details (Detalhes), em Instance details (Detalhes da instância), o campo Key pair name (Nome do par de chaves) exibe o nome do par de chaves especificado quando você executou a instância. O valor do Key pair name (Nome do par de chaves) não é alterado mesmo que você altere a chave pública na instância ou adicione pares de chaves.

Verificar a impressão digital do par de chaves

Na página Key Pairs (Pares de chaves) no console do Amazon EC2, a coluna Fingerprint (Impressão digital) exibe as impressões digitais geradas a partir de seus pares de chaves. A AWS calcula a impressão digital de forma diferente dependendo se o par de chaves foi gerado por AWS ou uma ferramenta de terceiros. Se você tiver criado o par de chaves usando a AWS, a impressão digital será calculada usando uma função hash SHA-1. Se você tiver criado o par de chaves com uma ferramenta de terceiros e

carregado a chave pública para a AWS, ou se tiver gerado uma nova chave pública a partir de uma chave privada criada pela AWS e carregado na AWS, a impressão digital será calculada usando uma função hash MD5.

Você pode usar a impressão digital SSH2 exibida na página Pares de chaves para verificar se a chave privada que você tem em sua máquina local corresponde à chave pública armazenada na AWS. Usando o computador em que o arquivo de chave privada foi obtido por download, gere uma impressão digital SSH2 a partir do arquivo de chave privada. A saída deve corresponder à impressão digital exibida no console.

Se estiver usando uma máquina local do Windows, poderá executar os comandos a seguir usando o Subsistema do Windows para Linux (WSL). Instale o WSL e uma distribuição do Linux usando as instruções do [Guia de instalação do Windows 10](#). O exemplo fornecido nas instruções instala a distribuição Ubuntu do Linux, mas você pode instalar qualquer distribuição. Você é solicitado a reiniciar o computador para que as alterações sejam implementadas.

Se você tiver criado o par de chaves usando a AWS, poderá usar as ferramentas OpenSSL para gerar uma impressão digital como no exemplo a seguir.

```
$ openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt | openssl sha1 -c
```

Se você tiver criado um par de chaves usando uma ferramenta de terceiros e feito upload da chave pública para a AWS, poderá usar as ferramentas OpenSSL para gerar a impressão digital da seguinte forma:

```
$ openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
```

Se tiver criado um par de chaves OpenSSH usando o OpenSSH 7.8 ou posterior e feito upload da chave pública para a AWS, você poderá usar ssh-keygen para gerar a impressão digital, como mostrado a seguir:

Para pares de chaves do RSA:

```
$ ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER | openssl md5 -c
```

Para pares de chaves ED25519:

```
$ ssh-keygen -l -f path_to_private_key.pem
```

Excluir o par de chaves

Ao excluir um par de chaves usando os métodos a seguir, você só exclui a chave pública que foi salva no Amazon EC2 quando você [criou \(p. 1210\)](#) ou [importou \(p. 1211\)](#) o par de chaves. A exclusão de um par de chaves não exclui a chave pública de nenhuma instância executada anteriormente usando esse par de chaves. Também não exclui a chave privada do computador local. Você pode continuar a se conectar a instâncias executadas usando um par de chaves excluído posteriormente, desde que ainda tenha a chave privada (.pem).

Se você estiver usando um grupo do Auto Scaling (por exemplo, em um ambiente do Elastic Beanstalk), verifique se o par de chaves que você está excluindo não está especificado em um modelo de execução associado ou configuração de execução. Se o Amazon EC2 Auto Scaling detectar uma instância não íntegra, executará uma instância de substituição. No entanto, o lançamento da instância falhará se o par de chaves não puder ser encontrado. Para obter mais informações, consulte [Launch templates \(Modelos de execução\)](#) no Amazon EC2 Auto Scaling User Guide (Guia do usuário do Amazon EC2 Auto Scaling).

Você pode excluir um par de chaves usando um dos seguintes métodos.

Console

Como excluir o par de chaves

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Key Pairs (Pares de chaves).
3. Selecione o par de chaves a ser excluído e escolha Delete (Excluir).
4. No campo de confirmação, insira Delete e escolha Delete (Excluir).

AWS CLI

Como excluir o par de chaves

Use o comando `delete-key-pair` da AWS CLI.

PowerShell

Como excluir o par de chaves

Use o comando `Remove-EC2KeyPair` do AWS Tools for Windows PowerShell.

Conectar-se à instância do Windows se você perder a chave privada

Quando você se conecta a uma instância do Windows recém-executada, você descriptografa a senha da conta do administrador usando a chave privada para o par de chaves que você especificou quando executou a instância.

Se você perder a senha do Administrador e não tiver mais a chave privada, é preciso redefinir a senha ou criar uma nova instância. Para obter mais informações, consulte [Redefinir uma senha de administrador do Windows perdida ou expirada \(p. 1590\)](#). Para conhecer as etapas e redefinir a senha usando o documento Systems Manager, consulte [Demonstração: redefinir senhas e chaves SSH nas instâncias do EC2](#) no Manual do usuário do AWS Systems Manager.

Grupos de segurança do Amazon EC2 para instâncias do Windows

Um grupo de segurança atua como firewall virtual para as instâncias do EC2 visando controlar o tráfego de entrada e de saída. As regras de entrada controlam o tráfego de entrada para a instância e as regras de saída controlam o tráfego de saída da instância. Ao executar sua instância, você pode especificar um ou mais grupos de segurança. Se você não especificar um grupo de segurança, o Amazon EC2 usará o grupo de segurança padrão. Você pode adicionar regras a cada grupo de segurança que permite tráfego de entrada ou de saída nas instâncias associadas. É possível modificar as regras de um grupo de segurança a qualquer momento. As regras novas e modificadas são aplicadas automaticamente para todas as instâncias que estão associados ao grupo de segurança. Quando o Amazon EC2 decide se deve permitir que o tráfego atinja uma instância, ele avalia todas as regras de todos os grupos de segurança associados à instância.

Ao executar uma instância em uma VPC, você precisa especificar um security group criado para a VPC. Depois de executar uma instância, você pode alterar seus security groups. Os security groups estão associados a interfaces de rede. A alteração dos security groups de uma instância altera os security groups associados à interface de rede primária (eth0). Para obter mais informações, consulte [Alterar os grupos de segurança de uma instância](#) no Guia do usuário da Amazon VPC. Você também pode alterar

os security groups associados a qualquer outra interface de rede. Para obter mais informações, consulte [Modificar atributos da interface de rede \(p. 1020\)](#).

A segurança é uma responsabilidade compartilhada entre a AWS e você. Para obter mais informações, consulte [Segurança no Amazon EC2 \(p. 1129\)](#). A AWS fornece grupos de segurança como uma das ferramentas para proteger as instâncias, e você precisa configurá-los para atender às suas necessidades de segurança. Se houver requisitos que não sejam totalmente atendidos pelos grupos de segurança, você pode manter seu próprio firewall em qualquer uma das instâncias além de usar grupos de segurança.

Para permitir o tráfego para uma instância do Linux, consulte [Grupos de segurança do Amazon EC2 para instâncias do Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Sumário

- [Regras de grupos de segurança \(p. 1218\)](#)
- [Rastreamento de conexão do grupo de segurança \(p. 1220\)](#)
 - [Conexões não rastreadas \(p. 1220\)](#)
 - [Example \(p. 1221\)](#)
 - [Throttling \(p. 1221\)](#)
- [Grupos de segurança padrão e personalizados \(p. 1222\)](#)
 - [Grupos de segurança padrão \(p. 1222\)](#)
 - [Os security groups personalizados \(p. 1223\)](#)
- [Trabalhar com grupos de segurança \(p. 1223\)](#)
 - [Crie um grupo de segurança \(p. 1223\)](#)
 - [Copiar um grupo de segurança \(p. 1224\)](#)
 - [Visualizar seus grupos de segurança \(p. 1225\)](#)
 - [Adicionar regras a um grupo de segurança \(p. 1226\)](#)
 - [Atualizar regras do grupo de segurança \(p. 1229\)](#)
 - [Excluir regras de um grupo de segurança \(p. 1230\)](#)
 - [Excluir um security group \(p. 1231\)](#)
 - [Atribuir um grupo de segurança a uma instância \(p. 1232\)](#)
 - [Para mudar o grupo de segurança de uma instância \(p. 1232\)](#)
- [Regras de grupo de segurança para diferentes casos de uso \(p. 1233\)](#)
 - [Regras do servidor da Web \(p. 1233\)](#)
 - [Regras do servidor de banco de dados \(p. 1234\)](#)
 - [Regras para conectar-se a instâncias pelo computador \(p. 1235\)](#)
 - [Regras para conectar-se a instâncias por uma instâncias com o mesmo grupo de segurança \(p. 1235\)](#)
 - [Regras de ping/ICMP \(p. 1236\)](#)
 - [Regras do servidor DNS \(p. 1236\)](#)
 - [Regras do Amazon EFS \(p. 1236\)](#)
 - [Regras do Elastic Load Balancing \(p. 1237\)](#)
 - [Regras de emparelhamento de VPC \(p. 1238\)](#)

Regras de grupos de segurança

As regras de um grupo de segurança controlam o tráfego de entrada que tem permissão para atingir as instâncias associadas ao grupo de segurança. As regras também controlam o tráfego de saída que pode deixá-los.

As seguintes são as características das regras de security groups:

- Por padrão, os security groups permitem todo o tráfego de saída. Observe que o Amazon EC2 bloqueia o tráfego na porta 25 por padrão. Para obter mais informações, consulte [Restrição para e-mails enviados usando a porta 25 \(p. 1568\)](#).
- As regras do security group sempre são permissivas. Você não pode criar regras que negam o acesso.
- As regras do grupo de segurança permitem filtrar o tráfego com base em protocolos e números de porta.
- Os grupos de segurança são stateful — se você enviar uma solicitação da instância, o tráfego da resposta dessa solicitação terá permissão para fluir, independentemente das regras de entrada do grupo de segurança. Para security groups da VPC, isso também significa que as respostas permitidas para o tráfego de entrada são permitidas para saída, independentemente das regras de saída. Para obter mais informações, consulte [Rastreamento de conexão do grupo de segurança \(p. 1220\)](#).
- Você pode adicionar e remover regras a qualquer momento. As novas regras são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança.

O efeito de algumas alterações nas regras pode depender de como o tráfego é acompanhado. Para obter mais informações, consulte [Rastreamento de conexão do grupo de segurança \(p. 1220\)](#).

- Quando você associa vários security groups a uma instância, as regras de cada security group são efetivamente agregadas para criar um conjunto de regras. O Amazon EC2 usa esse conjunto de regras para determinar se deve permitir acesso.

É possível atribuir vários grupos de segurança a uma instância. Portanto, uma instância pode ter centenas de regras aplicáveis. Isso pode causar problemas quando você acessar a instância. Recomendamos que você condense suas regras o máximo possível.

Ao criar o canal de entrega, é possível especificar as seguintes opções:

- Nome: o nome do grupo de segurança (por exemplo, “meu-grupo-de-segurança”).

Esse nome pode ter até 255 caracteres. Os caracteres permitidos são a-z, A-Z, 0-9, espaços e _-:/()#@[]+=;{}!\$*. Quando o nome contém espaços finais, cortamos os espaços ao salvá-lo. Por exemplo, se você inserir “Testar grupo de segurança ” para o nome, nós o armazenaremos como “Testar grupo de segurança”.

- Protocolo: o protocolo a permitir. Os protocolos mais comuns são 6 (TCP), 17 (UDP) e 1 (ICMP).
- Intervalo de portas: para TCP, UDP ou um protocolo personalizado, o intervalo de portas a ser permitido. Você pode especificar um único número de porta (por exemplo, 22) ou um intervalo de números de portas (por exemplo, 7000-8000).
- Tipo e código do ICMP: para o ICMP e ICMPv6, o tipo e o código do ICMP. Por exemplo, use o tipo 8 para solicitação de eco ICMP ou digite 128 para solicitação de eco ICMPv6.
- Origem ou destino: a origem (regras de entrada) ou o destino (regras de saída) para o tráfego. Especifique uma destas opções:
 - Um endereço IPv4 individual. Você deve usar o comprimento de prefixo /32; por exemplo, 203.0.113.1/32.
 - Um endereço IPv6 individual. Você deve usar o comprimento de prefixo /128; por exemplo, 2001:db8:1234:1a00::123/128.
 - Um intervalo de endereços IPv4, em notação de bloco CIDR. Por exemplo, 203.0.113.0/24.
 - Um intervalo de endereços IPv6, em notação de bloco CIDR. Por exemplo, 2001:db8:1234:1a00::/64.
 - Um ID de lista de prefixes, por exemplo, pl-1234abc1234abc123. Para obter mais informações, consulte [Listas de prefixes](#) no Guia do usuário da Amazon VPC.
- Outro security group. Isso permite que as instâncias associadas ao grupo de segurança especificado acessem instâncias associadas a esse grupo de segurança. Escolher essa opção não adiciona regras do grupo de segurança de origem a esse grupo de segurança. Você pode especificar um dos seguintes security groups:
 - O security group atual.
 - Um security group diferente para a mesma VPC

- Um security group diferente para uma VPC par em uma conexão de emparelhamento de VPC.
- (Opcional) Descrição: você pode adicionar uma descrição à regra, que pode ajudá-lo a identificá-la posteriormente. Uma descrição pode ser até 255 caracteres de comprimento. Os caracteres permitidos são a-z, A-Z, 0-9, espaços e ._-:/()#@[]+=;{}\$*.

Quando você cria uma regra de grupo de segurança, a AWS atribui um ID exclusivo à regra. Você pode usar o ID de uma regra ao usar a API ou a CLI para modificar ou excluir a regra.

Quando você especifica um grupo de segurança como a origem ou o destino de uma regra, a regra afeta todas as instâncias associadas ao grupo de segurança. O tráfego de entrada é permitido com base nos endereços IP privados das instâncias associadas ao security group de origem (e não aos endereços IP público ou IP elástico). Para obter mais informações sobre endereços IP, consulte [Endereçamento IP de instâncias do Amazon EC2 \(p. 956\)](#). Se a regra do security group fizer referência a um security group em uma VPC par, e o security group referenciado ou a conexão de emparelhamento da VPC for excluída, a regra será marcada como obsoleta. Para obter mais informações, consulte [Como trabalhar com regras de grupos de segurança obsoletas](#) no Amazon VPC Peering Guide.

Se houver mais de uma regra para uma porta específica, o Amazon EC2 aplicará a regra mais permissiva. Por exemplo, se você tiver uma regra que permita acesso à porta TCP 3389 (RDP) do endereço IP 203.0.113.1 e outra regra que permita acesso à porta TCP 3389 de todos, todos terão acesso à porta TCP 3389.

Quando você adiciona, atualiza ou remove regras, elas são aplicadas automaticamente a todas as instâncias associadas ao grupo de segurança.

Rastreamento de conexão do grupo de segurança

Os security groups usam o acompanhamento da conexão para acompanhar as informações sobre o tráfego de entrada e saída da instância. As regras são aplicadas com base no estado da conexão do tráfego para determinar se o tráfego é permitido ou negado. Com essa abordagem, os grupos de segurança são tipo com estado. Isso significa que as respostas ao tráfego de entrada têm permissão para sair da instância independentemente das regras do grupo de segurança de saída e vice-versa.

Por exemplo, suponha que você inicie um comando ping ICMP para instâncias de seu computador doméstico, e as regras de grupo de segurança de entrada permitem tráfego ICMP. As informações sobre a conexão (inclusive as informações da porta) são rastreadas. O tráfego de resposta da instância para o comando ping não é acompanhado como uma nova solicitação, mas sim como uma conexão estabelecida e tem permissão para sair da instância, mesmo que as regras de seu security group restrinjam o tráfego de saída ICMP.

Para protocolos diferentes de TCP, UDP ou ICMP, somente o endereço IP e o número do protocolo são acompanhados. Se a instância enviar tráfego para outro host (o host B), e o host B iniciar o mesmo tipo de tráfego para a instância em uma solicitação separada em 600 segundos após a solicitação original ou a resposta, a instância o aceitará independentemente das regras de entrada do grupo de segurança. A instância aceitará, pois será considerado como tráfego de resposta.

Para garantir que o tráfego seja interrompido imediatamente quando você remover uma regra de grupo de segurança, ou para garantir que todo o tráfego de entrada esteja sujeito às regras do firewall, você poderá usar uma Network ACL para a sub-rede. As Network ACLs são stateless e, portanto, não permitem automaticamente o tráfego de resposta. Para obter mais informações, consulte [Network ACLs](#) no Guia do usuário da Amazon VPC.

Conexões não rastreadas

Nem todos os fluxos de tráfego são acompanhados. Se uma regra do grupo de segurança permitir fluxos TCP ou UDP para todo o tráfego (0.0.0.0/0 ou ::/0) e houver uma regra correspondente na outra direção que permita todo o tráfego de resposta (0.0.0.0/0 ou ::/0) para todas as portas (0-65535), o fluxo do tráfego

não será rastreado. O fluxo do tráfego de resposta é permitido com base na regra de entrada ou de saída que permite o tráfego de resposta, e não nas informações de acompanhamento.

Um fluxo de tráfego não acompanhado será interrompido imediatamente se a regra que permite o fluxo for removida ou alterada. Por exemplo, se você tiver uma regra de saída aberta (0.0.0.0/0) e remover uma regra que permita todo tráfego (porta TCP 22) SSH de entrada (0.0.0.0/0) para a instância (ou modificá-la de forma que a conexão não seja mais permitida), suas conexões SSH existentes na instância serão imediatamente descartadas. A conexão não estava sendo rastreada anteriormente, então a alteração interromperá a conexão. Por outro lado, se você tiver uma regra de entrada mais restrita que inicialmente permita a conexão SSH (o que significa que a conexão foi rastreada), mas altere essa regra para não permitir mais novas conexões do endereço do cliente SSH atual, a conexão existente não será interrompida pela alteração da regra.

Example

No exemplo a seguir, o grupo de segurança tem regras de entrada específicas para tráfego TCP e ICMP, e regras de saída que permitem todo o tráfego de saída de IPv4 e IPv6.

Regras de entrada		
Tipo de protocolo	Número da porta	IP de origem
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	All	0.0.0.0/0

Regras de saída		
Tipo de protocolo	Número da porta	IP de destino
All	All	0.0.0.0/0
All	All	::/0

- O tráfego TCP na porta 22 (SSH) de entrada e saída da instância é rastreado, porque a regra de entrada permite o tráfego somente de 203.0.113.1/32, e não todos os endereços IP (0.0.0.0/0).
- O tráfego TCP na porta 80 (HTTP) de entrada e de saída da instância não é rastreado porque as regras de entrada e de saída permitem todo o tráfego (0.0.0.0/0 ou ::/0).
- O tráfego ICMP é sempre acompanhado, independentemente das regras.
- Se você remover a regra de saída do grupo de segurança, todo o tráfego de e para a instância será rastreado, incluindo o tráfego na porta 80 (HTTP).

Throttling

O Amazon EC2 define um número máximo de conexões que podem ser rastreadas por instância. Depois que o máximo é atingido, todos os pacotes enviados ou recebidos são descartados, porque não é possível estabelecer uma nova conexão. Quando isso acontece, as aplicações que enviam e recebem pacotes não podem se comunicar corretamente.

Para determinar se os pacotes foram descartados porque o tráfego de rede para sua instância excedeu o número máximo de conexões que podem ser rastreadas, use a métrica `conntrack_allowance_exceeded` de performance de rede. Para obter mais informações, consulte [Monitorar a performance de rede de sua instância do EC2 \(p. 1041\)](#).

As conexões feitas por meio de um平衡ador de carga da rede são rastreadas automaticamente, mesmo que a configuração do grupo de segurança não exija rastreamento. Caso exceda o número máximo de conexões que podem ser rastreadas por instância, recomendamos que você escala o número de instâncias registradas com o balanceador de carga ou o tamanho das instâncias registradas com o balanceador de carga.

Grupos de segurança padrão e personalizados

Sua conta da AWS tem automaticamente um grupo de segurança padrão para a VPC padrão em cada região. Se você não especificar um grupo de segurança ao executar uma instância, ela será associada automaticamente ao grupo de segurança padrão da VPC. Se não quiser que suas instâncias usem o grupo de segurança padrão, você poderá criar seus próprios grupos de segurança personalizados e especificá-los quando executar as instâncias.

Tópicos

- [Grupos de segurança padrão \(p. 1222\)](#)
- [Os security groups personalizados \(p. 1223\)](#)

Grupos de segurança padrão

Sua conta da AWS tem automaticamente um grupo de segurança padrão para a VPC padrão em cada região. Se você não especificar um grupo de segurança ao executar uma instância, ela será associada automaticamente ao grupo de segurança padrão da VPC.

Um grupo de segurança padrão é denominado “default” e tem um ID atribuído pela AWS. A tabela a seguir descreve as regras padrão para um security group padrão.

Regra de entrada			
Origem	Protocolo	Intervalo de portas	Descrição
O ID do grupo de segurança (seu próprio ID de recurso)	Tudo	Tudo	Permite tráfego de entrada de interfaces de rede e instâncias atribuídas ao mesmo grupo de segurança.
Regras de saída			
Destino	Protocolo	Intervalo de portas	Descrição
0.0.0.0/0	Tudo	Tudo	Permite todo o tráfego IPv4 de saída.
::/0	Tudo	Tudo	Permite todo o tráfego IPv6 de saída. Essa regra será adicionada somente se sua VPC tiver um bloco CIDR IPv6 associado.

Você pode adicionar ou remover as regras de entrada e saída para qualquer grupo de segurança padrão.

Você não pode excluir um security group padrão. Se tentar excluir o grupo de segurança padrão, você receberá o seguinte erro: `Client.CannotDelete: the specified group: "sg-51530134" name: "default" cannot be deleted by a user.`

Os security groups personalizados

Se não quiser que suas instâncias usem o security group padrão, você poderá criar seus próprios security groups e especificá-los ao executar as instâncias. Você pode criar vários security groups para refletir as diferentes funções que suas instâncias desempenham. Por exemplo, um servidor Web ou um servidor de banco de dados.

Ao criar um security group, você deve fornecer um nome e uma descrição. Os nomes e as descrições de security groups podem ter até 255 caracteres de comprimento e são limitados aos seguintes caracteres:

a-z, A-Z, 0-9, espaços e ._-:/()#,@[]+=;&{}!\$*

Um nome de grupo de segurança não pode começar com o seguinte: sg-. Um nome do grupo de segurança deve ser exclusivo da VPC.

As seguintes são as regras padrão para um security group que você cria:

- Não permite nenhum tráfego de entrada
- Permite todo o tráfego de saída

Depois de criar um security group, você pode alterar as regras de entrada para refletir o tipo de tráfego de entrada que você quer para atingir as instâncias associadas. Você também pode alterar as regras de saída.

Para obter mais informações sobre as regras que você pode adicionar a um grupo de segurança, consulte [Regras de grupo de segurança para diferentes casos de uso \(p. 1233\)](#).

Trabalhar com grupos de segurança

Você pode atribuir um security group a uma instância ao executá-la. Quando você adiciona ou remove regras, essas alterações são aplicadas automaticamente a todas as instâncias às quais você atribuiu o security group. Para obter mais informações, consulte [Atribuir um grupo de segurança a uma instância \(p. 1232\)](#).

Depois de executar uma instância, você pode alterar seus security groups. Para obter mais informações, consulte [Para mudar o grupo de segurança de uma instância \(p. 1232\)](#).

Você pode criar, visualizar, atualizar e excluir grupos de segurança e regras de grupos de segurança usando o console do Amazon EC2 e as ferramentas de linha de comando.

Tarefas

- [Crie um grupo de segurança \(p. 1223\)](#)
- [Copiar um grupo de segurança \(p. 1224\)](#)
- [Visualizar seus grupos de segurança \(p. 1225\)](#)
- [Adicionar regras a um grupo de segurança \(p. 1226\)](#)
- [Atualizar regras do grupo de segurança \(p. 1229\)](#)
- [Excluir regras de um grupo de segurança \(p. 1230\)](#)
- [Excluir um security group \(p. 1231\)](#)
- [Atribuir um grupo de segurança a uma instância \(p. 1232\)](#)
- [Para mudar o grupo de segurança de uma instância \(p. 1232\)](#)

Crie um grupo de segurança

Embora você possa usar o security group padrão para suas instâncias, é possível criar seus próprios grupos para refletir as diferentes funções que as instâncias desempenham no seu sistema.

Por padrão, novos grupos de segurança começam com apenas uma regra de saída que permite que todo o tráfego deixe as instâncias. Você deve adicionar regras para permitir qualquer tráfego de entrada ou para restringir o tráfego de saída.

Um grupo de segurança só pode ser usado na VPC na qual ele é criado.

New console

Para criar um security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha Create security group (Criar grupo de segurança).
4. Na seção Basic details (Detalhes básicos) faça o seguinte.
 - a. Insira um nome descritivo e uma breve descrição para o grupo de segurança. Eles não podem ser editados depois que o grupo de segurança é criado. O nome e a descrição podem ter até 255 caracteres. Os caracteres válidos são a-z, A-Z, 0-9, espaços e _:-/()#@[]+=&:{}!\$*.
 - b. Em VPC, escolha a VPC.
5. Você pode adicionar regras do grupo de segurança agora ou pode adicioná-las mais tarde. Para obter mais informações, consulte [Adicionar regras a um grupo de segurança \(p. 1226\)](#).
6. Você pode adicionar etiquetas agora ou pode adicioná-las mais tarde. Para adicionar uma tag, escolha Add new tag (Adicionar nova tag), e insira a chave e o valor da tag.
7. Escolha Create security group (Criar grupo de segurança).

Old console

Para criar um security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha Create Security Group.
4. Especifique um nome e uma descrição para o security group.
5. Para VPC, escolha o ID da VPC.
6. Você pode começar a adicionar regras ou escolher Create para criar o security group agora (você sempre pode adicionar regras mais tarde). Para obter mais informações sobre como adicionar regras, consulte [Adicionar regras a um grupo de segurança \(p. 1226\)](#).

Command line

Para criar um security group

Use um dos seguintes comandos:

- [create-security-group](#) (AWS CLI)
- [New-EC2SecurityGroup](#) (AWS Tools for Windows PowerShell)

Copiar um grupo de segurança

É possível criar um grupo de segurança com a cópia de um grupo existente. Ao copiar um grupo de segurança, a cópia tem as mesmas regras de entrada e saída que o grupo de segurança original. Se o

grupo de segurança original estiver em uma VPC, a cópia será criada na mesma VPC, a menos que você especifique uma diferente.

A cópia receberá um novo ID de grupo de segurança exclusivo e você deverá fornecer um nome a ela. Você também pode adicionar uma descrição.

Não é possível copiar um grupo de segurança de uma região para outra região.

É possível criar uma cópia de grupo de segurança personalizado usando um dos métodos a seguir.

New console

Para copiar um security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança a ser copiado e escolha Actions (Ações), Copy to new security group (Copiar para novo grupo de segurança).
4. Especifique um nome e uma descrição opcional e altere as regras da VPC e do grupo de segurança, se necessário.
5. Escolha Create (Criar).

Old console

Para copiar um security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o security group que deseja copiar, escolha Actions, Copy to new.
4. A caixa de diálogo Create Security Group é aberta e está preenchida com as regras do security group existente. Especifique um nome e uma descrição para o novo security group. Para VPC, escolha o ID da VPC. Depois de concluir, escolha Create.

Visualizar seus grupos de segurança

Você pode visualizar informações sobre seus grupos de segurança usando um dos seguintes métodos.

New console

Como visualizar seus grupos de segurança

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Seus grupos de segurança serão listados. Para exibir os detalhes de um grupo de segurança específico, incluindo suas regras de entrada e saída, escolha seu ID na coluna Security group ID (ID do grupo de segurança) .

Old console

Como visualizar seus grupos de segurança

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.

3. (Opcional) Selecione o ID de VPC da lista de filtro, e escolha o ID da VPC.
4. Selecione um security group. As informações gerais são exibidas na guia Description (Descrição), as regras de entrada na guia Inbound (Entrada), as regras de saída na guia Outbond (Saída) e tags na guia Tags.

Command line

Como visualizar seus grupos de segurança

Use um dos seguintes comandos.

- [describe-security-groups](#) (AWS CLI)
- [describe-security-group-rules](#) (AWS CLI)
- [Get-EC2SecurityGroup](#) (AWS Tools for Windows PowerShell)

Amazon EC2 Global View

Você pode usar o Amazon EC2 Global View para exibir seus grupos de segurança em todas as Regiões para as quais sua conta AWS está habilitada. Para obter mais informações, consulte [Listar e filtrar recursos entre Regiões usando o Amazon EC2 Global View \(p. 1553\)](#).

Adicionar regras a um grupo de segurança

Quando você adiciona uma regra a um grupo de segurança, a nova regra é aplicada automaticamente a todas as instâncias associadas ao grupo de segurança. Pode haver um pequeno atraso antes de a regra ser aplicada. Para obter mais informações, consulte [Regras de grupo de segurança para diferentes casos de uso \(p. 1233\)](#) e [Regras de grupos de segurança \(p. 1218\)](#).

New console

Como adicionar uma regra de entrada a um grupo de segurança

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha o grupo de segurança e selecione Actions(Ações), Edit inbound rules.(Editar regras de entrada).
4. Para cada regra, selecione Add Rule (Adicionar regra) e faça o seguinte.
 - a. Em Type (Tipo), escolha o tipo de protocolo a ser permitido.
 - Para TCP ou UDP personalizado, é necessário inserir o intervalo de portas que será permitido.
 - Para ICMP personalizado, você deverá escolher o nome do tipo ICMP em Protocolo e, se aplicável, o nome do código em Intervalo de portas. Por exemplo, para permitir comandos ping, escolha Solicitação eco de Protocolo.
 - Para qualquer outro tipo, o protocolo e o intervalo de portas serão configurados para você.
 - b. Em Source, (Origem), siga um dos procedimentos a seguir para permitir tráfego.
 - Escolha Custom (Personalizado) e insira um endereço IP na notação CIDR, um bloco CIDR, outro grupo de segurança ou uma lista de prefixos.
 - Escolha Anywhere (Qualquer lugar) para permitir que todo o tráfego de entrada do protocolo especificado alcance sua instância. Essa opção adiciona automaticamente o bloco CIDR IPv4 0.0.0.0/0 como origem. Isso é aceitável por um período curto em um ambiente de teste, porém não é seguro em ambientes de produção. No ambiente de

produção, autorize apenas um endereço IP específico ou um intervalo de endereços a acessar as instâncias.

Se o grupo de segurança estiver em uma VPC habilitada para IPv6, essa opção adicionará automaticamente uma regra para o bloco CIDR IPv6 ::/0.

- Escolha My IP (Meu IP) para permitir o tráfego de entrada somente do endereço IPv4 público do computador local.
- c. Em Description (Descrição), você pode especificar uma descrição para a regra.
- 5. Selecione Visualizar alterações, Salvar regras.

Como adicionar uma regra de saída a um grupo de segurança

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança e escolha Actions (Ações), Edit outbound rules (Editar regras de saída).
4. Para cada regra, selecione Add Rule (Adicionar regra) e faça o seguinte.
 - a. Em Type (Tipo), escolha o tipo de protocolo a ser permitido.
 - Para TCP ou UDP personalizado, é necessário inserir o intervalo de portas que será permitido.
 - Para ICMP personalizado, você deverá escolher o nome do tipo ICMP em Protocolo e, se aplicável, o nome do código em Intervalo de portas.
 - Para qualquer outro tipo, o protocolo e o intervalo de portas serão configurados automaticamente.
 - b. Em Destination (Destino), siga um dos procedimentos a seguir:
 - Escolha Personalizado e insira um endereço IP na notação CIDR, um bloco CIDR, outro grupo de segurança ou uma lista de prefixos para o qual permitir o tráfego de saída.
 - Escolha Anywhere (Qualquer lugar) para permitir o tráfego de saída para todos os endereços IP. Esta opção adiciona automaticamente o bloco CIDR IPv4 0.0.0.0/0 como destino.
 - c. (Opcional) Em Description (Descrição), especifique uma breve descrição para a regra.
5. Escolha Preview changes (Visualizar alterações), Confirm (Confirmar).

Old console

Para adicionar regras a um security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Security Groups e selecione o security group.
3. Na guia Entrada, escolha Editar.
4. Na caixa de diálogo, escolha Add Rule e faça o seguinte:
 - Em Type, selecione o protocolo.
 - Se você selecionar um protocolo TCP ou UDP personalizado, especifique o intervalo de portas em Port Range.

- Se você selecionar um protocolo ICMP personalizado, escolha o nome do tipo ICMP em Protocol e, se aplicável, o nome de código em Port Range. Por exemplo, para permitir comandos ping, escolha Solicitação eco de Protocolo.
- Em Source, escolha uma das seguinte opções:
 - Custom: no campo fornecido, você deve especificar um endereço IP em notação CIDR, um bloco CIDR ou outro security group.
 - Anywhere: adiciona automaticamente o bloco CIDR 0.0.0.0/0 IPv4. Essa opção permite que todo o tráfego do tipo especificado atinja a instância. Isso é aceitável para um período curto em um ambiente de teste, mas não é seguro em ambientes de produção. Em produção, autorize apenas um endereço IP específico ou um intervalo de endereços a acessar a instância.

Se o grupo de segurança estiver em uma VPC habilitada para IPv6, a opção Anywhere criará duas regras: uma para o tráfego IPv4 (0.0.0.0/0) e uma para o tráfego IPv6 (::/0).

- My IP: adiciona automaticamente o endereço IPv4 público do computador local.
- Para Descrição, você pode opcionalmente especificar uma descrição para a regra.

Para obter mais informações sobre os tipos de regras que você pode adicionar, consulte [Regras de grupo de segurança para diferentes casos de uso \(p. 1233\)](#).

5. Escolha Save (Salvar).
6. Você também pode especificar regras de entrada e saída. Na Outbound tab, escolha Editar, Add Rule e faça o seguinte:
 - Em Type, selecione o protocolo.
 - Se você selecionar um protocolo TCP ou UDP personalizado, especifique o intervalo de portas em Port Range.
 - Se você selecionar um protocolo ICMP personalizado, escolha o nome do tipo ICMP em Protocol e, se aplicável, o nome de código em Port Range.
 - Em Destination, escolha uma das seguintes opções:
 - Custom: no campo fornecido, você deve especificar um endereço IP em notação CIDR, um bloco CIDR ou outro security group.
 - Anywhere: adiciona automaticamente o bloco CIDR 0.0.0.0/0 IPv4. Essa opção permite tráfego de saída para todos os endereços IP.
7. Se o grupo de segurança estiver em uma VPC habilitada para IPv6, a opção Anywhere criará duas regras: uma para o tráfego IPv4 (0.0.0.0/0) e uma para o tráfego IPv6 (::/0).
 - My IP: adiciona automaticamente o endereço IP do computador local.
 - Para Descrição, você pode opcionalmente especificar uma descrição para a regra.
7. Escolha Save (Salvar).

Command line

Para adicionar regras a um security group

Use um dos seguintes comandos.

- [authorize-security-group-ingress](#) (AWS CLI)
- [Grant-EC2SecurityGroupIngress](#) (AWS Tools for Windows PowerShell)

Como adicionar uma ou mais regras de saída a um grupo de segurança

Use um dos seguintes comandos.

- [authorize-security-group-egress](#) (AWS CLI)
- [Grant-EC2SecurityGroupEgress](#) (AWS Tools for Windows PowerShell)

Atualizar regras do grupo de segurança

É possível atualizar uma regra de grupo de segurança usando um dos seguintes métodos. A regra atualizada é aplicada automaticamente a todas as instâncias associadas ao grupo de segurança.

New console

Quando você modifica o protocolo, o intervalo de portas ou a origem ou o destino de um security group existente usando o console, o console exclui a regra existente e adiciona uma nova para você.

Como atualizar uma regra de grupo de segurança

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o security group.
4. Escolha Actions (Ações) e Edit inbound rules (Editar regras de entrada) para atualizar uma regra para tráfego de entrada ou Actions e Edit outbound rules (Editar regras de saída) para atualizar uma regra para tráfego de saída.
5. Atualize a regra conforme necessário.
6. Escolha Preview changes (Visualizar alterações), Confirm (Confirmar).

Para etiquetar uma regra do grupo de segurança

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o security group.
4. Na guia Inbound rules (Regras de entrada) ou Outbound rules (Regras de saída), marque a caixa de seleção da regra e escolha Manage tags (Gerenciar tags).
5. A seção Manage tags (Gerenciar tags) exibe todas as tags atribuídas à regra. Para adicionar uma tag, escolha Add tag (Adicionar tag), e insira a chave e o valor da tag. Para excluir uma tag, escolha Remove (Remover) ao lado da tag que você deseja excluir.
6. Selecione Save changes (Salvar alterações).

Old console

Quando você modifica o protocolo, o intervalo de portas ou a origem ou o destino de um security group existente usando o console, o console exclui a regra existente e adiciona uma nova para você.

Como atualizar uma regra de grupo de segurança

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Escolha o grupo de segurança a ser atualizado e selecione a guia Entrada, para atualizar uma regra para o tráfego de entrada, ou a guia Saída, para atualizar uma regra para o tráfego de saída.
4. Selecione Edit.
5. Modifique entrada de regra conforme necessário e escolha Save.

Command line

Não é possível modificar o protocolo, o intervalo de portas ou a origem ou o destino de uma regra existente usando a API do Amazon EC2 ou uma ferramenta de linha de comando. Em vez disso, você deve excluir a regra existente e adicionar uma regra nova. No entanto, você pode atualizar a descrição de uma regra existente.

Para atualizar uma regra

Use um dos comandos a seguir.

- [modify-security-group-rules](#) (AWS CLI)

Como atualizar a descrição de uma regra de entrada existente

Use um dos seguintes comandos.

- [update-security-group-rule-descriptions-ingress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleIngressDescription](#) (AWS Tools for Windows PowerShell)

Como atualizar a descrição de uma regra de saída existente

Use um dos seguintes comandos.

- [update-security-group-rule-descriptions-egress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleEgressDescription](#) (AWS Tools for Windows PowerShell)

Para etiquetar uma regra do grupo de segurança

Use um dos seguintes comandos.

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)

Excluir regras de um grupo de segurança

Quando você excluir uma regra de um security group, a alteração é aplicada automaticamente a todas as instâncias associadas ao security group.

É possível excluir regras de um grupo de segurança usando um dos métodos a seguir.

New console

Para excluir uma regra de security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança a ser atualizado, escolha Actions (Ações) e Edit inbound rules (Editar regras de entrada) para remover uma regra de entrada ou Edit outbound rules (Editar regras de saída) para remover uma regra de saída.
4. Escolha o botão Delete (Excluir) à direita da regra que será excluída.
5. Escolha Preview changes (Visualizar alterações), Confirm (Confirmar).

Old console

Para excluir uma regra de security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione um security group.
4. Na guia Inbound (para regras de entrada) ou na guia Outbound (para regras de saída), escolha Edit. Escolha Delete (um ícone de cruz) ao lado de cada regra a ser excluída.
5. Escolha Save (Salvar).

Command line

Como remover uma ou mais regras de entrada de um grupo de segurança

Use um dos seguintes comandos.

- [revoke-security-group-ingress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupIngress](#) (AWS Tools for Windows PowerShell)

Como remover uma ou mais regras de saída de um grupo de segurança

Use um dos seguintes comandos.

- [revoke-security-group-egress](#) (AWS CLI)
- [Revoke-EC2SecurityGroupEgress](#) (AWS Tools for Windows PowerShell)

Excluir um security group

Você não pode excluir um security group que esteja associado a uma instância. Você não pode excluir o security group padrão. Você não pode excluir um security group referenciado por uma regra em outro security group na mesma VPC. Se o security group for referenciado por uma de suas próprias regras, você deverá excluir a regra para poder excluir o security group.

New console

Para excluir um security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione o grupo de segurança a ser excluído, e Actions (Ações), Delete security group (Excluir grupo de segurança), Delete (Excluir).

Old console

Para excluir um security group

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Grupos de segurança.
3. Selecione um security group e escolha Actions, Delete Security Group.
4. Selecione Sim, excluir.

Command line

Para excluir um security group

Use um dos seguintes comandos.

- [delete-security-group](#) (AWS CLI)
- [Remove-EC2SecurityGroup](#) (AWS Tools for Windows PowerShell)

Atribuir um grupo de segurança a uma instância

Você pode atribuir um ou mais grupos de segurança a uma instância quando executá-la. Você também pode especificar um ou mais grupos de segurança em um modelo de execução. Os grupos de segurança serão atribuídos a todas as instâncias que são executadas usando o modelo de execução.

- Para atribuir um grupo de segurança a uma instância ao executá-la, consulte [Etapa 6: configurar o grupo de segurança \(p. 424\)](#).
- Para especificar um grupo de segurança em um modelo de execução, consulte Etapa 6 de [Criar um novo modelo de execução usando parâmetros definidos \(p. 427\)](#).

Para mudar o grupo de segurança de uma instância

Depois de executar uma instância, você pode mudar os grupos de segurança dela adicionando ou removendo grupos de segurança. Você pode mudar os grupos de segurança quando a instância está no estado `running` ou `stopped`.

New console

Para alterar os grupos de segurança de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, em seguida, escolha Actions (Ações), Security (Segurança), Change security groups (Mudar grupos de segurança).
4. Em Associated security groups (Grupos de segurança associados), selecione um grupo de segurança na lista e escolha Add security group (Adicionar grupo de segurança).

Para remover um grupo de segurança já associado, escolha Remove (Remover) para esse grupo de segurança.

5. Escolha Save (Salvar).

Old console

Para alterar os grupos de segurança de uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e, em seguida, escolha Actions (Ações), Networking (Redes), Change security groups (Mudar grupos de segurança).
4. Para adicionar um ou mais grupos de segurança, marque a caixa de seleção correspondente.

Para remover um grupo de segurança já associado, desmarque a caixa de seleção.

5. Escolha Assign Security Groups.

Command line

Para alterar os grupos de segurança de uma instância usando a linha de comando

Use um dos seguintes comandos.

- [modify-instance-attribute](#) (AWS CLI)
- [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

Regras de grupo de segurança para diferentes casos de uso

Você pode criar um security group e adicionar regras que refletem a função da instância associada ao security group. Por exemplo, uma instância configurada como servidor Web precisa de regras de grupo de segurança que permitam acesso HTTP e HTTPS de entrada. Da mesma forma, uma instância de banco de dados precisa de regras que permitam o acesso para o tipo de banco de dados, como acesso pela porta 3306 para MySQL.

Os seguintes são exemplos de tipos de regras que você pode adicionar aos security groups para tipos específicos de acesso.

Exemplos

- [Regras do servidor da Web](#) (p. 1233)
- [Regras do servidor de banco de dados](#) (p. 1234)
- [Regras para conectar-se a instâncias pelo computador](#) (p. 1235)
- [Regras para conectar-se a instâncias por uma instâncias com o mesmo grupo de segurança](#) (p. 1235)
- [Regras de ping/ICMP](#) (p. 1236)
- [Regras do servidor DNS](#) (p. 1236)
- [Regras do Amazon EFS](#) (p. 1236)
- [Regras do Elastic Load Balancing](#) (p. 1237)
- [Regras de emparelhamento de VPC](#) (p. 1238)

Regras do servidor da Web

As seguintes regras de entrada permitem acesso HTTP e HTTPS de qualquer endereço IP. Se a VPC estiver habilitada para IPv6, você poderá adicionar regras para controlar o tráfego de entrada HTTP e HTTPS em endereços IPv6.

Tipo de protocolo	Número do protocolo	Porta	IP de origem	Observações
TCP	6	80 (HTTP)	0.0.0.0/0	Permite acesso HTTP de entrada em qualquer endereço IPv4
TCP	6	443 (HTTPS)	0.0.0.0/0	Permite acesso HTTPS de entrada em qualquer endereço IPv4
TCP	6	80 (HTTP)	::/0	Permite acesso HTTP de entrada em qualquer endereço IPv6

Tipo de protocolo	Número do protocolo	Porta	IP de origem	Observações
TCP	6	443 (HTTPS)	::/0	Permite acesso HTTPS de entrada em qualquer endereço IPv6

Regras do servidor de banco de dados

As seguintes regras de entrada são exemplos de regras que você pode adicionar para acesso ao banco de dados, dependendo do tipo de banco de dados que você está executando na instância. Para obter mais informações sobre instâncias do Amazon RDS, consulte o [Manual do usuário do Amazon RDS](#).

Para o IP de origem, especifique um dos seguintes:

- Um endereço IP específico ou um intervalo de endereços IP (na notação de bloco CIDR) em sua rede local
- Um ID de security group para um grupo de instâncias que acessa o banco de dados

Tipo de protocolo	Número do protocolo	Porta	Observações
TCP	6	1433 (MS SQL)	A porta padrão para acessar um banco de dados Microsoft SQL Server, por exemplo, em uma instância do Amazon RDS
TCP	6	3306 (MySQL/Aurora)	A porta padrão para acessar um banco de dados MySQL ou Aurora, por exemplo, em uma instância do Amazon RDS
TCP	6	5439 (Redshift)	A porta padrão para acessar um banco de dados de cluster do Amazon Redshift.
TCP	6	5432 (PostgreSQL)	A porta padrão para acessar um banco de dados PostgreSQL, por exemplo, em uma instância do Amazon RDS
TCP	6	1521 (Oracle)	A porta padrão para acessar um banco de dados Oracle, por exemplo, em uma instância do Amazon RDS

Também é possível restringir o tráfego de saída de seus servidores de banco de dados. Por exemplo, talvez você queira permitir o acesso à Internet para atualizações de software, mas restringir todos os outros tipos de tráfego. Primeiro, você deve remover a regra de saída padrão que permite todo o tráfego de saída.

Tipo de protocolo	Número do protocolo	Porta	IP de destino	Observações
TCP	6	80 (HTTP)	0.0.0.0/0	Permite acesso HTTP de saída a qualquer endereço IPv4

Tipo de protocolo	Número do protocolo	Porta	IP de destino	Observações
TCP	6	443 (HTTPS)	0.0.0.0/0	Permite acesso HTTPS de saída a qualquer endereço IPv4
TCP	6	80 (HTTP)	::/0	(VPC habilitada para IPv6 somente) Permite acesso de saída HTTP a qualquer endereço IPv6
TCP	6	443 (HTTPS)	::/0	(VPC habilitada para IPv6 somente) Permite acesso de saída HTTPS a qualquer endereço IPv6

Regras para conectar-se a instâncias pelo computador

Para conectar-se à instância, seu security group deve ter regras de entrada que permitam acesso SSH (para instâncias do Linux) ou acesso RDP (para instâncias do Windows).

Tipo de protocolo	Número do protocolo	Porta	IP de origem
TCP	6	22 (SSH)	O endereço IPv4 público de seu computador ou um intervalo de endereços IP na rede local. Se a VPC estiver habilitada para IPv6 e sua instância tiver um endereço IPv6, você poderá digitar um endereço IPv6 ou um intervalo.
TCP	6	3389 (RDP)	O endereço IPv4 público de seu computador ou um intervalo de endereços IP na rede local. Se a VPC estiver habilitada para IPv6 e sua instância tiver um endereço IPv6, você poderá digitar um endereço IPv6 ou um intervalo.

Regras para conectar-se a instâncias por uma instâncias com o mesmo grupo de segurança

Para permitir que as instâncias associadas ao mesmo security group se comuniquem entre si, você deve adicionar regras explícitas para isso.

A tabela a seguir descreve a regra de entrada para um security group que permite que as instâncias associadas se comuniquem entre si. A regra permite todos os tipos de tráfego.

Tipo de protocolo	Número do protocolo	Portas	IP de origem
-1 (todos)	-1 (todos)	-1 (todos)	O ID do security group.

Regras de ping/ICMP

O comando ping é um tipo de tráfego ICMP. Para executar ping na instância, você deve adicionar a seguinte regra de entrada ICMP.

Tipo de protocolo	Número do protocolo	Tipo ICMP	Código ICMP	IP de origem
ICMP	1	8 (Solicitação eco)	N/D	O endereço IPv4 público de seu computador ou um intervalo de endereços IPv4 na rede local.

Para usar o comando ping6 para fazer ping no endereço IPv6 da instância, você deve adicionar a seguinte regra ICMPv6 de entrada.

Tipo de protocolo	Número do protocolo	Tipo ICMP	Código ICMP	IP de origem
ICMPv6	58	128 (Solicitação eco)	0	O endereço IPv6 público de seu computador ou um intervalo de endereços IPv6 na rede local.

Regras do servidor DNS

Se tiver configurado a instância do EC2 como um servidor DNS, você deverá garantir que o tráfego TCP e UDP possa atingir seu servidor DNS pela porta 53.

Para o IP de origem, especifique um dos seguintes:

- Um endereço IP ou um intervalo de endereços IP (na notação de bloco CIDR) em uma rede
- O ID de um security group de um conjunto de instâncias na rede que requer acesso ao servidor DNS

Tipo de protocolo	Número do protocolo	Porta
TCP	6	53
UDP	17	53

Regras do Amazon EFS

Se estiver usando um sistema de arquivos do Amazon EFS com instâncias do Amazon EC2, o grupo de segurança que você associa a seus destinos de montagem do Amazon EFS deve permitir tráfego por meio do protocolo NFS.

Tipo de protocolo	Número do protocolo	Portas	IP de origem	Observações
TCP	6	2049 (NFS)	O ID do security group	Permite acesso NFS de entrada de recursos

Tipo de protocolo	Número do protocolo	Portas	IP de origem	Observações
				(incluindo o destino de montagem) associados a esse grupo de segurança

Para montar um sistema de arquivos do Amazon EFS na instância do Amazon EC2, você deve se conectar à instância. Portanto, o security group associado à instância deve ter regras que permitam SSH de entrada do computador local ou da rede local.

Tipo de protocolo	Número do protocolo	Portas	IP de origem	Observações
TCP	6	22 (SSH)	O intervalo de endereços IP do computador local ou o intervalo de endereços IP (na notação de bloco CIDR) da rede.	Permite acesso SSH de entrada no computador local.

Regras do Elastic Load Balancing

Se você estiver usando um load balancer, o security group associado ao load balancer deve ter regras que permitam comunicação com suas instâncias ou destinos.

Entrada				
Tipo de protocolo	Número do protocolo	Porta	IP de origem	Observações
TCP	6	The listener port	Para um load balancer voltado para a Internet: 0.0.0.0/0 (todos os endereços IPv4)	Allow inbound traffic on the load balancer listener port.
			Para um load balancer interno: o bloco CIDR IPv4 da VPC	
Saída				
Tipo de protocolo	Número do protocolo	Porta	IP de destino	Observações
TCP	6	The instance listener port	The ID of the instance security group	Allow outbound traffic to instances on the instance listener port.
TCP	6	The health check port	The ID of the instance security group	Allow outbound traffic to instances on the health check port.

As regras do security group para suas instâncias devem permitir que o load balancer se comunique com as instâncias na porta do ouvinte e na porta de verificação de integridade.

Entrada				
Tipo de protocolo	Número do protocolo	Porta	IP de origem	Observações
TCP	6	The instance listener port	O ID do load balancer do security group	Allow traffic from the load balancer on the instance listener port.
TCP	6	The health check port	The ID of the load balancer security group	Allow traffic from the load balancer on the health check port.

Para obter mais informações, consulte [Configurar grupos de segurança para o Classic Load Balancer](#) em Guia do usuário para Classic Load Balancers e [Grupos de segurança para o Balanceador de carga de aplicações](#) no Guia do usuário para Application Load Balancers.

Regras de emparelhamento de VPC

Você pode atualizar as regras de entrada e saída dos security groups de VPC para referenciar security groups na VPC emparelhada. Fazendo isso, você permite que o tráfego fluia entre as instâncias associadas com o security group referenciado na VPC emparelhada. Para obter mais informações sobre como configurar grupos de segurança para emparelhamento de VPC, consulte [Atualizar os grupos de segurança para referenciar grupos de VPC de mesmo nível](#).

Gerenciamento de configuração no Amazon EC2

As imagens de máquina da Amazon (AMIs) fornecem uma configuração inicial para uma instância do Amazon EC2, que inclui o sistema operacional Windows e personalizações opcionais específicas do cliente, como aplicações e controles de segurança. Crie um catálogo de AMIs contendo linhas de base de configuração de segurança personalizadas para garantir que todas as instâncias do Windows sejam executadas com controles de segurança padrão. As linhas de base de segurança podem ser incorporadas em uma AMI, inicializadas dinamicamente quando uma instância do EC2 é executada ou empacotadas como um produto para distribuição uniforme por meio de portfólios do AWS Service Catalog. Para obter mais informações sobre como proteger uma AMI, consulte [Práticas recomendadas para criar uma AMI](#).

Cada instância do Amazon EC2 deve aderir aos padrões de segurança organizacional. Não instale nenhuma função e recurso do Windows que não seja necessário e instale software (antivírus, antimalware, mitigação de vulnerabilidades) para proteger contra códigos mal-intencionados, monitore a integridade do host e execute a detecção de intrusões. Configure o software de segurança para monitorar e manter as configurações de segurança do SO, proteger a integridade de arquivos críticos do SO e alertar sobre desvios da linha de base de segurança. Considere implementar benchmarks recomendados de configuração de segurança publicados pela Microsoft, pelo Centro de Segurança da Internet (CIS) ou pelo National Institute of Standards and Technology (NIST). Considere usar outras ferramentas da Microsoft para servidores de aplicações específicos, como o [Analizador de melhores práticas para SQL Server](#).

Os clientes da AWS também podem executar avaliações do Amazon Inspector para aprimorar a segurança e a conformidade das aplicações implantadas nas instâncias do Amazon EC2. O Amazon Inspector avalia automaticamente as aplicações quanto a vulnerabilidades ou desvios das práticas recomendadas e inclui

uma base de conhecimento de centenas de regras mapeadas para padrões comuns de conformidade de segurança (por exemplo, PCI DSS) e definições de vulnerabilidade. Exemplos de regras incorporadas incluem verificar se o início remoto de sessão raiz está habilitado ou se versões de software vulneráveis estão instaladas. Essas regras são atualizadas regularmente pelos pesquisadores de segurança da AWS.

Gerenciamento de atualizações no Amazon EC2

Recomendamos corrigir, atualizar e proteger regularmente o sistema operacional e as aplicações em suas instâncias do EC2. É possível usar o [Gerenciador de patches do AWS Systems Manager](#) para automatizar o processo de instalação de atualizações relacionadas à segurança para o sistema operacional e para a aplicação. Como alternativa, é possível usar qualquer serviço de atualização automática ou processos recomendados para instalar atualizações fornecidas pelo fornecedor da aplicação.

Configure o Windows Update em suas instâncias do Amazon EC2 executando o Windows Server. Por padrão, você não receberá atualizações do Windows em AMIs fornecidas pela AWS. Para obter uma lista das AMIs do Amazon EC2 mais recentes que executam o Windows Server, consulte [Details About AWS Windows AMI Versions \(Detalhes sobre as versões da AMI do Windows da AWS\)](#).

Gerenciamento de alterações no Amazon EC2

Depois que as linhas de base de segurança iniciais forem aplicadas às instâncias do Amazon EC2 durante a execução, controle as alterações contínuas do Amazon EC2 para manter a segurança das máquinas virtuais. Estabeleça um processo de gerenciamento de alterações para autorizar e incorporar alterações aos recursos da AWS (como grupos de segurança, tabelas de rotas e ACLs de rede), bem como a configurações do SO e de aplicações (como aplicação de patches do Windows ou da aplicação, atualizações de software ou atualizações de arquivos de configuração).

A AWS fornece várias ferramentas para ajudar a gerenciar alterações nos recursos da AWS, incluindo o AWS CloudTrail, o AWS Config, o AWS CloudFormation, o AWS Elastic Beanstalk, o AWS OpsWorks, e pacotes de gerenciamento para o Systems Center Operations Manager e o System Center Virtual Machine Manager. Observe que a Microsoft libera patches do Windows todas as terças-feiras (às vezes até diariamente) e a AWS atualiza todas as AMIs do Windows gerenciadas pela AWS dentro de cinco dias após a Microsoft liberar um patch. Portanto, é importante corrigir continuamente todas as AMIs de linha de base, atualizar modelos do AWS CloudFormation e configurações de grupo de Auto Scaling com os IDs de AMI mais recentes e implementar ferramentas para automatizar o gerenciamento de patches de instâncias em execução.

A Microsoft fornece várias opções para gerenciar o sistema operacional Windows e as alterações de aplicações. O SCCM, por exemplo, fornece cobertura completa do ciclo de vida das modificações do ambiente. Selecione ferramentas que atendam aos requisitos comerciais e controlem como as alterações afetarão os SLAs de aplicações, a capacidade, a segurança e os procedimentos de recuperação de desastres. Evite alterações manuais e, em vez disso, utilize o software de gerenciamento de configuração automatizado ou ferramentas de linha de comando, como o Run Command do EC2 ou o Windows PowerShell, para implementar processos de alteração com script e repetíveis. Para ajudar com esse requisito, use bastion hosts com registro em log aprimorado para todas as interações com suas instâncias do Windows para garantir que todos os eventos e tarefas sejam gravados automaticamente.

Validação de conformidade do Amazon EC2

Auditores externos avaliam a segurança e a conformidade dos serviços da AWS como parte de vários programas de conformidade da AWS, como SOC, PCI, FedRAMP e HIPAA.

Para saber se a Amazon Elastic Compute Cloud ou outros produtos da AWS estão no escopo de programas de conformidade específicos, consulte [AWS Services in Scope by Compliance Program \(Produtos da AWS no escopo por programa de conformidade\)](#). Para obter informações gerais, consulte [Programas de conformidade da AWS](#).

Você pode fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte [Fazer download de relatórios no AWS Artifact](#).

Sua responsabilidade com relação à conformidade ao usar os serviços da AWS é determinada pela confidencialidade dos dados, pelos objetivos de conformidade da empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar com a conformidade:

- [Guias de referência rápida de conformidade e segurança](#): esses guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de lista de referência na AWS concentrados em conformidade e segurança.
- [Whitepaper Arquitetura para segurança e conformidade com a HIPAA](#): esse whitepaper descreve como as empresas podem usar a AWS para criar aplicações em conformidade com a HIPAA.

Note

Nem todos os serviços estão em conformidade com a HIPAA.

- [Recursos de conformidade da AWS](#): essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- [Avaliar recursos com regras](#) no AWS Config Developer Guide (Guia do desenvolvedor do AWS Config): o serviço AWS Config avalia como as configurações de recursos estão em conformidade com práticas internas, diretrizes do setor e regulamentos.
- [AWS Security Hub](#): esse serviço da AWS fornece uma visão abrangente do estado de sua segurança na AWS que ajuda você a verificar sua conformidade com padrões e práticas recomendadas de segurança do setor.
- [AWS Audit Manager](#): esse serviço da AWS ajuda a auditar continuamente o uso da AWS para simplificar a forma como você gerencia os riscos e a conformidade com regulamentos e padrões do setor.

O Amazon EC2 fornece imagens de máquina da Amazon (AMIs) para o Microsoft Windows Server para ajudar você a atender aos padrões de conformidade do Security Technical Implementation Guide (STIG - Guia de implementação técnica de segurança). As AMIs são pré-configuradas com vários padrões do STIG para ajudar você a começar a usar suas implantações atendendo aos padrões de conformidade do STIG. Para obter mais informações, consulte [AMIs do Amazon EC2 Windows Server para conformidade com STIG \(p. 56\)](#).

Auditoria e responsabilidade no Amazon EC2

O AWS CloudTrail, o AWS Config e o AWS Config Rules fornecem recursos de auditoria e controle de alterações para a auditoria de alterações de recursos da AWS. Configure os logs de eventos do Windows para enviar arquivos de log locais a um sistema centralizado de gerenciamento de logs a fim de preservar os dados de log para a análise de comportamento operacional e de segurança. O Microsoft System Center Operations Manager (SCOM) agrupa informações sobre aplicações da Microsoft implantadas em instâncias do Windows e aplica conjuntos de regras pré-configurados e personalizados com base em funções e serviços de aplicações. Os Pacotes de Gerenciamento do System Center são baseados no SCOM para fornecer monitoramento e orientações de configuração específicos da aplicação. Esses [Pacotes de Gerenciamento](#) oferecem suporte ao Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014 e muitos mais servidores e tecnologias. O AWS Management Pack para Microsoft System Center Operations Manager (SCOM) e o Systems Manager para Microsoft System Center Virtual Machine Manager (SCVMM) integram-se ao Microsoft Systems Center para ajudar você a monitorar e gerenciar seus ambientes locais e da AWS juntos.

Além das ferramentas de gerenciamento de sistemas da Microsoft, os clientes podem usar o Amazon CloudWatch para monitorar a utilização da CPU da instância, a performance do disco, a E/S da rede e realizar verificações de status do host e da instância. Os serviços EC2Config e EC2Launch fornecem acesso a recursos adicionais e avançados para instâncias do Windows. Por exemplo, eles podem exportar logs do sistema, de segurança, de aplicações e de Serviços de Informações da Internet (IIS) do Windows para o CloudWatch Logs, os quais poderão ser integrados a métricas e alarmes do Amazon CloudWatch. Os clientes também podem criar scripts que exportam contadores de performance do Windows para métricas personalizadas do Amazon CloudWatch.

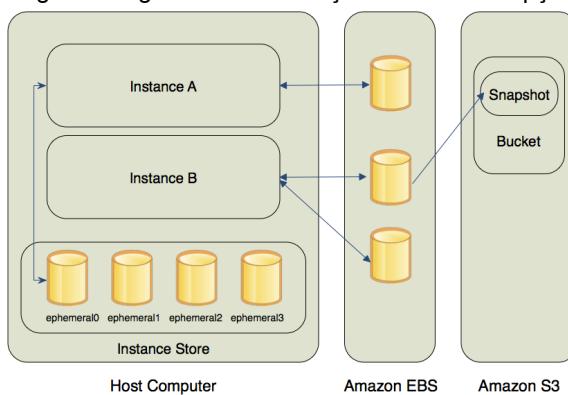
Storage

O Amazon EC2 fornece opções de armazenamento físico de dados flexíveis, econômicas e fáceis de usar para suas instâncias. Cada opção tem uma combinação exclusiva de performance e durabilidade. Essas opções de armazenamento podem ser usadas independentemente ou em conjunto para atender às suas necessidades.

Depois de ler esta seção, você deve ter uma boa compreensão de como usar as opções de armazenamento físico de dados suportadas pelo Amazon EC2 para atender aos requisitos específicos. Essas opções de armazenamento incluem o seguinte:

- [Amazon Elastic Block Store \(p. 1243\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#)
- [Usar o Amazon S3 com a Amazon EC2 \(p. 1504\)](#)

A figura a seguir mostra a relação entre essas opções de armazenamento e sua instância.



Amazon EBS

O Amazon EBS fornece volumes de armazenamento em bloco duráveis que podem ser anexados a uma instância em execução. Você pode usar o Amazon EBS como um dispositivo de armazenamento principal para dados que exigem atualizações frequentes e granulares. Por exemplo, o Amazon EBS é a opção de armazenamento recomendada para executar um banco de dados em uma instância.

Um volume do EBS comporta-se como um dispositivo de bloco externo, não formatado e bruto que você pode anexar a uma única instância. O volume é mantido independentemente da vida útil de uma instância. Depois de anexar um volume do EBS a uma instância, você poderá usá-lo como qualquer outro disco rígido físico. Conforme ilustrado na figura anterior, vários volumes podem ser anexados a uma instância. Você também pode desanexar um volume do EBS de uma instância e anexá-lo a outra instância. Você pode alterar dinamicamente a configuração de um volume anexado a uma instância. Os volumes do EBS também podem ser criados como volumes criptografados usando o recurso Criptografia de Amazon EBS. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).

Para manter uma cópia de backup de seus dados, você pode criar um snapshot de um volume do EBS, que é armazenado no Amazon S3. Também é possível criar um novo volume do EBS de um snapshot e anexá-lo a outra instância. Para obter mais informações, consulte [Amazon Elastic Block Store \(p. 1243\)](#).

Armazenamento de instâncias do Amazon EC2

Muitas instâncias podem acessar o armazenamento em discos anexados fisicamente ao computador host. Esse armazenamento em disco é denominado armazenamento de instâncias. O armazenamento de instâncias fornece armazenamento temporário em nível de bloco para as instâncias. Os dados em um volume de armazenamento de instâncias só são mantidos durante a vida da instância associada; se

você interromper, hibernar ou encerrar uma instância, todos os dados em volumes de armazenamento de instâncias serão perdidos. Para obter mais informações, consulte [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#).

Amazon S3

O Amazon S3 fornece acesso a uma infraestrutura de armazenamento físico de dados confiável e econômica. Ele foi projetado para facilitar a computação em escala da Web habilitando o armazenamento e a recuperação de qualquer quantidade de dados, a qualquer momento, no Amazon EC2 ou em qualquer lugar na Web. Por exemplo, você pode usar o Amazon S3 para armazenar cópias de backup de seus dados e aplicações. O Amazon EC2 usa o Amazon S3 para armazenar snapshots do EBS e AMIs com armazenamento de instâncias. Para obter mais informações, consulte [Usar o Amazon S3 com a Amazon EC2 \(p. 1504\)](#).

Adicionar armazenamento

Sempre que você executa uma instância a partir de uma AMI, um dispositivo de armazenamento raiz é criado para essa instância. O dispositivo de armazenamento raiz contém todas as informações necessárias para inicializar a instância. Você pode especificar volumes de armazenamento além do volume de dispositivo raiz quando você cria uma AMI ou executa uma instância usando mapeamento de dispositivos de bloco. Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1513\)](#).

Você também pode anexar volumes do EBS a uma instância em execução. Para obter mais informações, consulte [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#).

Definição de preço de armazenamento

Para obter informações sobre definição de preço de armazenamento, abra [Definição de preço da AWS](#), role para baixo até Services Pricing (Definição de preço de serviços), escolha Storage (Armazenamento) e, depois, escolha a opção de armazenamento para abrir a página de definição de preço dela. Para obter informações sobre como estimar o custo do armazenamento, consulte a [AWS Pricing Calculator \(Calculadora de definição de preço da AWS\)](#).

Amazon Elastic Block Store (Amazon EBS)

O Amazon Elastic Block Store (Amazon EBS) oferece volumes de armazenamento em bloco para usar com instâncias do EC2. Os volumes do EBS se comportam como dispositivos de bloco brutos e não formatados. Você pode montar esses volumes como dispositivos em suas instâncias. Os volumes EBS que estão anexados a uma instância são expostos como volumes de armazenamento que persistem independentemente da vida útil da instância. Você pode criar um sistema de arquivos sobre esses volumes ou utilizá-los da maneira que utilizaria um dispositivo de bloco (como um disco rígido). Você pode alterar dinamicamente a configuração de um volume anexado a uma instância.

O Amazon EBS é recomendado para dados que devem ser rapidamente acessíveis e requerem persistência no longo prazo. Os volumes do EBS são especialmente adequados ao uso como armazenamento principal para sistemas de arquivos, bancos de dados ou para todas as aplicações que necessitem de atualizações granulares finas e acesso ao armazenamento em nível de bloco bruto e não formatado. O Amazon EBS é ideal para aplicações no estilo de banco de dados que utilizam leituras e gravações aleatórias, bem como para aplicações com alta taxa de transferência que executam leituras e gravações longas e contínuas.

Com o Amazon EBS, você paga somente por aquilo que usa. Para obter mais informações sobre a definição de preço do Amazon EBS, consulte a seção de Projeção de custos da [página do Amazon Elastic Block Store](#).

Tópicos

- [Recursos do Amazon EBS \(p. 1244\)](#)
- [Volumes do Amazon EBS \(p. 1245\)](#)

- [Snapshots do Amazon EBS \(p. 1294\)](#)
- [Amazon Data Lifecycle Manager \(p. 1363\)](#)
- [Serviços de dados do Amazon EBS \(p. 1409\)](#)
- [Amazon EBS e NVMe em instâncias Windows \(p. 1438\)](#)
- [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#)
- [Performance de volume do Amazon EBS em instâncias Windows \(p. 1458\)](#)
- [Métricas do Amazon CloudWatch para o Amazon EBS \(p. 1472\)](#)
- [Amazon CloudWatch Events para Amazon EBS \(p. 1479\)](#)
- [Cotas do Amazon EBS \(p. 1490\)](#)

Recursos do Amazon EBS

- Você cria um volume do EBS em uma zona de disponibilidade específica e, em seguida, o anexa a uma instância nessa mesma zona de disponibilidade. Para tornar um volume disponível fora da zona de disponibilidade, você pode criar um snapshot e restaurá-lo em um novo volume em qualquer lugar nessa região. Você pode copiar os snapshots para outras regiões e então restaurá-los para novos volumes nelas, viabilizando o aproveitamento de várias regiões da AWS para expansão geográfica, migração de datacenter e a recuperação de desastres.
- O Amazon EBS fornece os seguintes tipos de volumes: SSD de uso geral, SSD com IOPS provisionadas, HDD otimizado para taxa de transferência e HDD a frio. Para obter mais informações, consulte [Tipos de volume do EBS \(p. 1247\)](#).

A seguir está um resumo da performance e dos casos de uso de cada tipo de volume.

- Os volumes SSD de uso geral (gp2 e gp3) equilibram preço e performance para uma ampla variedade de workloads transacionais. Esses volumes são ideais para casos de uso, como volumes de inicialização, bancos de dados de instância única de tamanho médio e ambientes de desenvolvimento e teste.
- Os volumes SSD de IOPS provisionadas (io1 e io2) são criados para atender às necessidades de workloads com uso intensivo de E/S que são sensíveis a performance e consistência de armazenamento. Fornecem uma taxa de IOPS consistente que você especifica ao criar o volume. Isso permite que você escala de forma previsível para dezenas de milhares de IOPS por instância. Além disso, os volumes io2 fornecem os mais altos níveis de durabilidade de volume.
- Os volumes HDD otimizados para taxa de transferência (st1) fornecem armazenamento magnético de baixo custo que define a performance em termos de taxa de transferência, não IOPS. Esses volumes são ideais para workloads grandes e sequenciais, como Amazon EMR, ETL, data warehouses e processamento de logs.
- Os volumes de HDD (sc1) fornecem armazenamento magnético de baixo custo que define a performance em termos de taxa de transferência, não IOPS. Esses volumes são ideais para workloads grandes, sequenciais e cold data. Se você precisar acesso infrequente aos dados e estiver em busca de economia de custos, esses volumes fornecerão armazenamento econômico em blocos.
- Você pode criar seus volumes de EBS na forma de volumes criptografados, a fim de atingir uma ampla série de requisitos de criptografia de dados em repouso para dados e aplicações regulamentados/auditados. Quando você cria um volume do EBS criptografado e o anexa a um tipo de instância com suporte, os dados armazenados em repouso no volume, E/S de disco e snapshots criados do volume são todos criptografados. A criptografia ocorre nos servidores que hospedam as instâncias do EC2, processando-se durante o trânsito dos dados entre as instâncias do EC2 e o armazenamento no EBS. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).
- Você pode criar snapshots de pontos no tempo dos volumes do EBS, que são persistidos no Amazon S3. Os snapshots protegem os dados para durabilidade de longo prazo, e eles podem ser usados como ponto inicial para novos volumes do EBS. O mesmo snapshot pode ser usado para criar quantos volumes você quiser. Esses snapshots podem ser copiados nas regiões da AWS. Para obter mais informações, consulte [Snapshots do Amazon EBS \(p. 1294\)](#).

- As métricas de performance, como a largura de banda, a taxa de transferência, a latência e o tamanho da fila média, estão disponíveis por meio do AWS Management Console. Essas métricas, fornecidas pelo Amazon CloudWatch, permitem que você monitore a performance de seus volumes para garantir que você forneça performance suficiente para suas aplicações sem pagar por recursos de que não precisa. Para obter mais informações, consulte [Performance de volume do Amazon EBS em instâncias Windows \(p. 1458\)](#).

Volumes do Amazon EBS

Um volume do Amazon EBS é um dispositivo de armazenamento em blocos durável que você pode anexar às suas instâncias. Depois de anexar um volume a uma instância, será possível usá-lo como você usaria um disco rígido físico. Os volumes do EBS são flexíveis. Para volumes de geração atual anexados a tipos de instância de geração atual, você pode aumentar o tamanho dinamicamente, modificar a capacidade de IOPS provisionadas e alterar o tipo de volume em volumes de produção em tempo real.

Você pode usar os volumes do EBS como armazenamento principal de dados que exigem atualizações frequentes, como o drive do sistema para uma instância ou armazenamento de uma aplicação de banco de dados. Você também pode usá-los para aplicações com muita taxa de transferência que executam verificações de disco contínuas. Os volumes do EBS persistem independentemente da vida útil de uma instância do EC2.

É possível anexar vários volumes do EBS a uma única instância. O volume e a instância devem estar na mesma zona de disponibilidade.

O Amazon EBS fornece os seguintes tipos de volumes: SSD de uso geral (gp2 e gp3), SSD de IOPS provisionadas (io1 e io2), HDD otimizado para taxa de transferência (st1), HDD a frio (sc1) e Magnético (standard). Eles diferem em características de performance e preço, permitindo que você adapte a performance e custo de armazenamento às necessidades das aplicações. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#).

Sua conta tem um limite no número de volumes do EBS que você pode usar, e no armazenamento total disponível para você. Para obter mais informações sobre esses limites e como solicitar um aumento, consulte [Cotas de serviço do Amazon EC2 \(p. 1567\)](#).

Para obter mais informações sobre definição de preço, consulte [Definição de preço do Amazon EBS](#).

Tópicos

- [Benefícios de usar volumes do EBS \(p. 1245\)](#)
- [Tipos de volume do Amazon EBS \(p. 1247\)](#)
- [Restrições de tamanho e configuração de um volume do EBS \(p. 1265\)](#)
- [Crie um volume do Amazon EBS. \(p. 1268\)](#)
- [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#)
- [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#)
- [Visualizar informações sobre um volume do Amazon EBS \(p. 1276\)](#)
- [Substituir um volume do Amazon EBS \(p. 1278\)](#)
- [Monitorar o status de seus volumes \(p. 1282\)](#)
- [Desanexar um volume do Amazon EBS de uma instância Windows \(p. 1290\)](#)
- [Excluir um volume de Amazon EBS \(p. 1293\)](#)

Benefícios de usar volumes do EBS

Os volumes do EBS fornecem benefícios que não são fornecidos por volumes de armazenamento de instâncias.

Disponibilidade de dados

Ao criar um volume do EBS, ele será automaticamente replicado dentro da zona de disponibilidade para evitar perda de dados devido à falha de qualquer componente de hardware único. É possível anexar um volume do EBS a qualquer instância do EC2 na mesma zona de disponibilidade. Depois de associar um volume, ele será exibido como um dispositivo de blocos nativo semelhante a um disco rígido ou a outro dispositivo físico. A partir desse momento, a instância pode interagir com o volume da mesma forma que faria com uma unidade local. É possível se conectar à instância e formatar o volume do EBS com um sistema de arquivos, como NTFS, e instalar aplicações.

Se você associar vários volumes a um dispositivo ao qual deu o nome, pode distribuir os dados pelos volumes para maior performance de E/S e taxa de transferência.

Você pode obter dados de monitoramento para seus volumes do EBS, inclusive volumes do dispositivo raiz para instâncias com EBS, sem custo adicional. Para obter mais informações sobre as métricas de monitoramento, consulte [Métricas do Amazon CloudWatch para o Amazon EBS \(p. 1472\)](#). Para obter informações sobre como acompanhar o status de seus volumes, consulte [Amazon CloudWatch Events para Amazon EBS \(p. 1479\)](#).

Persistência de dados

Um volume do EBS é um armazenamento fora da instância capaz de persistir independentemente da duração de uma instância. Você continua a pagar pela utilização do volume, desde que os dados persistam.

Os volumes do EBS que são anexados a uma instância em execução poderão ser desanexados automaticamente da instância com os dados intactos quando a instância for encerrada, se você desmarcar a caixa de seleção `Delete on Termination` (Excluir no encerramento) ao configurar volumes do EBS para a instância no console do EC2. O volume pode então ser reassociado a uma nova instância, permitindo a rápida recuperação. Se a caixa de seleção de `Delete on Termination` (Excluir no encerramento) estiver marcada, os volumes serão excluídos no encerramento da instância do EC2. Se você estiver usando uma instância com EBS, poderá pará-la e reiniciá-la sem afetar os dados armazenados no volume associado. O volume permanece associado durante todo o ciclo de parada-início. Isso permite que você processe e armazene os dados no seu volume indefinidamente, usando os recursos de processamento e armazenamento apenas conforme necessário. Os dados persistirão no volume até que o volume seja excluído explicitamente. O armazenamento de blocos físicos usados pelos volumes do EBS é substituído por zeros antes que ser alocado para outra conta. Se você estiver lidando com dados confidenciais, deve considerar criptografar seus dados manualmente ou armazenar dados em um volume protegido pelo Criptografia de Amazon EBS. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).

Por padrão, o volume raiz do EBS criado e associado a uma instância em execução é excluído quando essa instância é encerrada. Você pode modificar esse comportamento alterando o valor do marcador `DeleteOnTermination` para `false` ao executar a instância. Esse valor modificado faz com que o volume persista mesmo após a instância ser encerrada e permite associar o volume a outra instância.

Por padrão, os volumes adicionais do EBS criados e associados a uma instância em execução não são excluídos quando essa instância é encerrada. Você pode modificar esse comportamento alterando o valor do marcador `DeleteOnTermination` para `true` ao executar a instância. Esse valor modificado faz com que o volume seja excluído quando a instância é encerrada.

Criptografia de dados

Para criptografia simplificada de dados, você pode criar volumes do EBS criptografados com o recurso Criptografia de Amazon EBS. Todos os tipos de volume do EBS são compatíveis com criptografia. Você pode usar volumes de EBS criptografados para atingir uma ampla série de requisitos de criptografia de dados em repouso para dados e aplicações regulamentados/auditados. A criptografia do Amazon EBS

usa algoritmos do Advanced Encryption Standard de 256 bits (AES-256) e uma infraestrutura de chaves gerenciada pela Amazon. A criptografia ocorre no servidor que hospeda a instância do EC2, fornecendo criptografia dos dados em trânsito desde a instância do EC2 até o armazenamento Amazon EBS. Para obter mais informações, consulte [Criptografia da Amazon EBS \(p. 1422\)](#).

A criptografia do Amazon EBS usa chaves mestras do AWS Key Management Service (AWS KMS) ao criar volumes criptografados e quaisquer snapshots criados a partir dos seus volumes criptografados. Na primeira vez que você criar um volume do EBS criptografado em uma região, será criada automaticamente uma chave mestra padrão. Essa chave é usada para o criptografia de Amazon EBS, a menos que você selecione uma chave mestra de cliente (CMK) criada separadamente usando o AWS KMS. Criar sua própria CMK oferece mais flexibilidade, inclusive a capacidade de criar, rotacionar, desativar e definir controles de acesso, além de auditar as chaves de criptografia usadas para proteger seus dados. Para obter mais informações, consulte o [Guia do desenvolvedor do AWS Key Management Service](#).

Snapshots

O Amazon EBS oferece a capacidade de criar snapshots (backups) de qualquer volume do EBS e gravar uma cópia dos dados no volume para o Amazon S3, onde ele é armazenado repetidamente em várias zonas de disponibilidade. O volume não precisa estar anexado a uma instância em execução para obter um snapshot. À medida que você continua a gravar dados a um volume, pode periodicamente criar um snapshot do volume para usar como linha de base para novos volumes. Esses snapshots podem ser usados para criar vários novos volumes do EBS ou mover volumes entre zonas de disponibilidade. Os snapshots de volumes do EBS criptografados são automaticamente criptografados também.

Ao criar um novo volume a partir de um snapshot, ele será uma cópia exata do volume original no momento em que o snapshot foi tirado. Os volumes do EBS criados de snapshots criptografados são criptografados automaticamente. Ao especificar opcionalmente uma zona de disponibilidade diferente, você pode usar essa funcionalidade para criar uma duplicata do volume nessa zona. Os snapshots podem ser compartilhados com contas específicas da AWS ou serem públicos. Ao criar snapshots, serão feitas cobranças no Amazon S3 com base no tamanho total do volume. Para um snapshot sucessivo do volume, só será cobrado de você pelos dados adicionais além do tamanho do volume original.

Snapshots são backups incrementais, o que significa que serão salvos somente os blocos no volume que mudaram depois de o snapshot mais recente. Se você tiver um volume com 100 GiB de dados, mas somente 5 GiB de dados tiverem mudado desde seu último snapshot, somente os 5 GiB de dados modificados serão gravados em Amazon S3. Mesmo que os snapshots sejam salvos de forma incremental, o processo de exclusão de snapshots foi projetado de forma que você precise manter somente o snapshot mais recente.

Para ajudar a categorizar e gerenciar seus volumes e snapshots, você pode marcá-los com os metadados de sua escolha. Para obter mais informações, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

Para fazer backup de seus volumes automaticamente, é possível usar [Amazon Data Lifecycle Manager \(p. 1363\)](#) ou o [AWS Backup](#).

Flexibility

Os volumes do EBS oferecem suporte a alterações de configuração reais durante a produção. Você pode modificar o tipo de volume, o tamanho e a capacidade de IOPS sem interrupções de serviço. Para obter mais informações, consulte [Volumes elásticos do Amazon EBS \(p. 1409\)](#).

Tipos de volume do Amazon EBS

O Amazon EBS fornece os tipos de volume a seguir, que diferem em características de performance e preço, de forma que você adapte o custo e a performance de armazenamento às necessidades das aplicações. Os tipos de volumes se encaixam nestas categorias:

- **Unidades de estado sólido (SSD) (p. 1248)** — otimizadas para workloads de transação envolvendo operações de leitura/gravação frequentes com o tamanho pequeno de E/S, onde o atributo dominante de performance é IOPS.
- **Unidades de disco rígido (HDD) (p. 1249)**: otimizadas para grandes workloads de transmissão em que o atributo de performance dominante é a taxa de transferência.
- **Geração anterior (p. 1250)** — unidades de disco rígido que podem ser usadas para workloads com pequenos conjuntos de dados em que os dados são acessados raramente e a performance não é de primordial importância. Recomendamos considerar um tipo de volume de geração atual.

Há vários fatores que podem afetar a performance dos volumes do EBS, como a configuração da instância, as características de E/S e a demanda das workloads. Para usar totalmente as IOPS provisionadas em um volume do EBS, use [instâncias otimizadas para EBS \(p. 1440\)](#). Para obter mais informações sobre como aproveitar ao máximo seus volumes do EBS, consulte [Performance de volume do Amazon EBS em instâncias Windows \(p. 1458\)](#).

Para obter mais informações sobre definição de preço, consulte [Definição de preço do Amazon EBS](#).

Unidades de estado sólido (SSD)

Os volumes com SSD fornecidos pelo Amazon EBS se enquadram nas seguintes categorias:

- Finalidade geral (SSD) — fornece um equilíbrio entre preço e performance. Recomendamos esses volumes para a maioria das workloads.
- Provisioned IOPS SSD — fornece alta performance para workloads de missão crítica, de baixa latência ou de alta taxa de transferência.

Segue-se um resumo dos casos de uso e características dos volumes suportados por SSD. Para obter informações sobre o máximo de IOPS e a taxa de transferência por instância, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

	General Purpose SSD		Provisioned IOPS SSD		
Tipo de volume	gp3	gp2	io2 Block Express ‡	io2	io1
Durabilidade	99,8% a 99,9% de durabilidade (taxa anual de falhas de 0,1% a 0,2%)	99,8% a 99,9% de durabilidade (taxa anual de falhas de 0,1% a 0,2%)	Durabilidade de 99,999% (taxa anual de falhas de 0,001%)	Durabilidade de 99,999% (taxa anual de falhas de 0,001%)	99,8% a 99,9% de durabilidade (taxa anual de falhas de 0,1% a 0,2%)
Casos de uso	<ul style="list-style-type: none">• Aplicações interativas de baixa latência• Ambientes de teste e desenvolvimento	Workloads que exigem: <ul style="list-style-type: none">• Latência média abaixo de um milissegundo• Performance estável de IOPS• Mais de 64.000 IOPS ou 1.000 MiB/	<ul style="list-style-type: none">• Workloads que exigem performance de IOPS sustentado ou mais do que 16.000 IOPS• Workloads de banco de dados com alto consumo de E/S		

	General Purpose SSD		Provisioned IOPS SSD	
			s de taxa de transferência	
Tamanho do volume	1 GiB – 16 TiB		4 GiB – 64 TiB	4 GiB – 16 TiB
Máximo de IOPS por volume (16 KiB E/S)	16.000		256.000	64.000 †
Taxa de transferência máxima por volume	1.000 MiB/s	250 MiB/s *	4.000 MiB/s	1.000 MiB/s †
Multi-attach do Amazon EBS	Não suportado		Compatível	
Volume de inicialização	Compatível			

* O limite de taxa de transferência é entre 128 MiB/s e 250 MiB/s, dependendo do tamanho do volume. Volumes menores ou iguais a 170 GiB fornecem uma taxa de transferência máxima de 128 MiB/s. Os volumes maiores que 170 GiB e menores que 334 GiB fornecerão uma taxa de transferência máxima de 250 MiB/s se houver créditos de intermitência disponíveis. Volumes maiores ou iguais a 334 GiB fornecem 250 MiB/s independentemente dos créditos de intermitência. Volumes gp2 criados antes de 3 de dezembro de 2018 e que não foram modificados desde a criação podem não atingir a performance total, a menos que você [modifique o volume \(p. 1409\)](#).

† O número máximo de IOPS e a taxa de transferência são garantidos somente em [Instâncias criadas no Sistema Nitro \(p. 154\)](#) provisionadas com mais de 32.000 IOPS. Outras instâncias garantem até 32.000 IOPS e 500 MiB/s. Volumes io1 criados antes de 6 de dezembro de 2017 e que não foram modificados desde a criação podem não atingir a performance total, a menos que você [modifique o volume \(p. 1409\)](#).

‡ Os volumes io2 do Block Express são compatíveis apenas com instâncias R5b. Volumes io2 anexados a uma instância R5b durante ou após a inicialização são executados automaticamente no Block Express. Para obter mais informações, consulte [Volumes io2 do Block Express \(p. 1256\)](#).

Unidades de disco rígido (HDD)

Os volumes com HDD fornecidos pelo Amazon EBS se enquadram nestas categorias:

- HDD otimizado para taxa de transferência: um HDD de baixo custo criado para workloads acessadas com frequência e com altas taxas de transferência.

- HDD a frio: o design de HDD de menor custo para workloads acessadas com menos frequência.

Segue um resumo dos casos de uso e características dos volumes suportados por HDD. Para obter informações sobre o máximo de IOPS e a taxa de transferência por instância, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

	HDD otimizado para taxa de transferência	Disco rígido frio
Tipo de volume	st1	sc1
Durabilidade	99,8% a 99,9% de durabilidade (taxa anual de falhas de 0,1% a 0,2%)	99,8% a 99,9% de durabilidade (taxa anual de falhas de 0,1% a 0,2%)
Casos de uso	<ul style="list-style-type: none">• Big data• Data warehouses• Processamento de logs	<ul style="list-style-type: none">• Armazenamento orientado para taxa de transferência para dados acessados raramente• Cenários nos quais o menor custo de armazenamento é importante
Tamanho do volume	125 GiB – 16 TiB	125 GiB – 16 TiB
Máximo de IOPS por volume (1 MiB E/S)	500	250
Taxa de transferência máxima por volume	500 MiB/s	250 MiB/s
Multi-attach do Amazon EBS	Não suportado	Não suportado
Volume de inicialização	Não suportado	Não suportado

Tipos de volumes da geração anterior

A tabela a seguir descreve os tipos de volumes do EBS de geração anterior. Se você precisar de performance superior ou de uma consistência de performance superior à dos volumes da geração anterior, recomendamos que use SSD de uso geral (gp2 e gp3) ou outros tipos atuais de volume. Para obter mais informações, consulte [Volumes da geração anterior](#).

	Magnético
Tipo de volume	standard
Casos de uso	Workloads nas quais os dados são acessados raramente
Tamanho do volume	1 GiB-1 TiB
IOPS máxima por volume	40 a 200
Taxa de transferência máxima por volume	40 a 90 MiB/s

	Magnético
Volume de inicialização	Compatível

Volumes Finalidade geral (SSD) (gp3)

Os volumes SSD de uso geral (gp3) oferecem armazenamento econômico ideal para uma ampla variedade de workloads. Esses volumes oferecem uma taxa de base consistente de 3.000 IOPS e 125 MiB/s, incluindo o preço do armazenamento. Você pode provisionar IOPS adicionais (até 16.000) e taxa de transferência (até 1.000 MiB/s) por um custo adicional.

A proporção máxima de IOPS provisionadas para o tamanho do volume provisionado é de 500 IOPS por GiB. A proporção máxima de taxa de transferência provisionada para IOPS provisionadas é de 0,25 MiB/s por IOPS. As seguintes configurações de volume suportam o provisionamento de IOPS máximo ou taxa de transferência máxima:

- 32 GiB ou maior: 500 IOPs/GiB x 32 GiB = 16.000 IOPS
- 8 GiB ou maior e 4.000 IOPS ou superior: 4.000 IOPS x 0,25 MiB/s/IOPs = 1.000 MiB/s

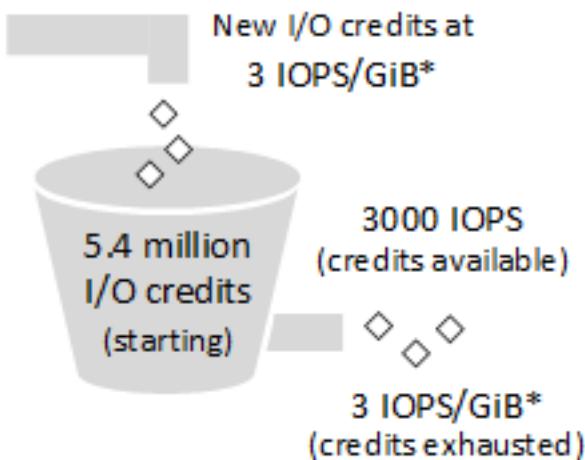
Volumes de Finalidade geral (SSD) (gp2)

Os volumes SSD de uso geral (gp2) oferecem armazenamento econômico ideal para uma ampla variedade de workloads. Esses volumes fornecem latências de milissegundo com único dígito e capacidade de intermitência a 3.000 IOPS por períodos de tempo prolongados. Entre um mínimo de 100 IOPS (a 33,33 GiB ou menos) e um máximo de 16.000 IOPS (a 5.334 GiB ou mais), a performance básica faz uma escala linear a 3 IOPS por GiB de tamanho do volume. A AWS projeta volumes gp2 para entregar a performance provisionada em 99% do tempo. O volume do gp2 pode variar de tamanho entre 1 GiB e 16 TiB.

Créditos de E/S e performance de intermitência

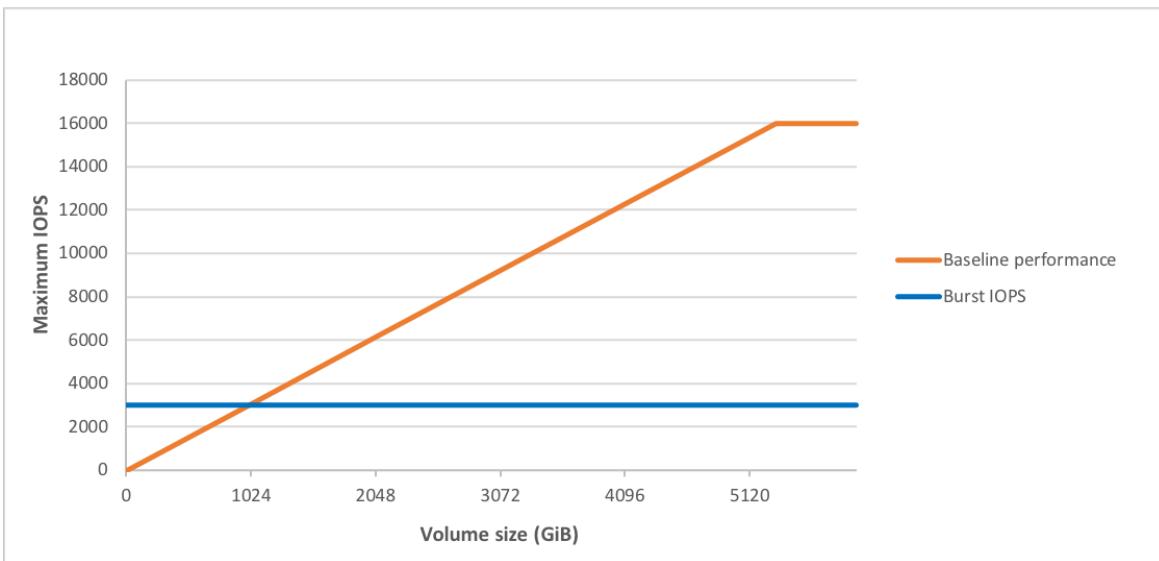
A performance dos volumes de gp2 é vinculada ao tamanho do volume, que determina o nível de performance basal do volume e a rapidez com que acumula créditos de E/S; volumes maiores têm níveis de performance basais mais altos e acumulam créditos de E/S com maior rapidez. Os créditos de E/S representam a largura de banda disponível que seu volume de gp2 pode usar para usar a intermitência de grandes quantidades de E/S quando mais performance basal for necessário. Quanto mais créditos seu volume tiver para E/S, mais tempo ele poderá ter intermitência além do nível de performance basal e melhor será a performance quando mais performance for necessária. O diagrama a seguir mostra comportamento do bucket de intermitência para gp2.

GP2 burst bucket



* Scaling linearly between minimum 100 IOPS and maximum 16,000 IOPS

Cada volume recebe um saldo de crédito de E/S inicial de 5,4 milhões de créditos de E/S, que é suficiente para sustentar a performance máxima de intermitência de 3.000 IOPS por pelo menos 30 minutos. O saldo de crédito inicial é projetado para fornecer um ciclo de inicialização inicial rápido para volumes de inicialização e fornecer uma boa experiência de bootstrapping para outras aplicações. Os volumes ganham créditos de E/S na taxa de performance basal de 3 IOPS por GiB de tamanho do volume. Por exemplo, um volume de gp2 de 100 GiB tem uma performance basal de 300 IOPS.



Quando seu volume exigir mais que o nível de E/S de performance basal, ele recorrerá a créditos de E/S no saldo de crédito para fazer a intermitência no nível de performance desejado, até o máximo de 3.000 IOPS. Quando seu volume usar menos créditos de E/S que ganhar em um segundo, os créditos não utilizados de E/S são adicionados ao saldo de crédito de E/S. O saldo de crédito de E/S máximo para um volume é igual ao saldo de crédito inicial (5,4 milhões de créditos de E/S).

Quando a performance basal de um volume for maior que a performance de intermitência máxima, os créditos de E/S nunca serão gastos. Se o volume estiver anexado a uma instância criada no [Sistema Nitro](#) (p. 154), o equilíbrio de intermitência não será relatado. Para outras instâncias, o equilíbrio de intermitência relatado é de 100%.

A duração da intermitência de um volume depende do tamanho do volume, do IOPS de intermitência necessário e do equilíbrio de crédito quando a intermitência iniciar. Isso é mostrado na equação a seguir:

$$\text{Burst duration} = \frac{\text{(Credit balance)}}{(\text{Burst IOPS}) - 3(\text{Volume size in GiB})}$$

A tabela a seguir apresenta vários tamanhos de volume e a performance basal associada do volume (que também é a taxa na qual ele acumula créditos de E/S), a duração de intermitência em 3.000 IOPS no máximo (ao começar com um saldo de crédito total) e o tempo, em segundos, que o volume demoraria para encher novamente um saldo de crédito vazio.

Tamanho do volume (GiB)	Performance basal (IOPS)	Duração da intermitência sustentando 3.000 IOPS (segundo)	Segundos para preencher o saldo de crédito vazio sem gerar E/S
1	100	1.802	54.000
100	300	2.000	18.000
250	750	2.400	7.200
334 (tamanho mín. para taxa de transferência máx.)	1.002	2.703	5.389
500	1.500	3.600	3.600
750	2.250	7.200	2.400
1.000	3.000	N/D*	N/D*
5.334 (tamanho mín. para IOPS máx.)	16.000	N/D*	N/D*
16.384 (16 TiB, máx. tamanho de volume)	16.000	N/D*	N/D*

* A performance basal do volume excede a performance de intermitência máxima.

O que acontece se esvaziar meu saldo de crédito de E/S?

Se seu volume do gp2 usar todo o saldo de crédito de E/S, a performance máxima de IOPS do volume permanecerá no nível de performance basal de IOPS (a taxa em que seu volume ganha créditos) e a taxa de transferência máxima do volume será reduzida para IOPS basal multiplicado pelo tamanho de E/S máximo. A taxa de transferência nunca pode exceder 250 MiB/s. Quando a demanda de E/S cair abaixo do nível basal e os créditos não utilizados forem adicionados ao saldo de crédito de E/S, a performance máxima de IOPS do volume novamente excederá a linha de base. Por exemplo, um volume de gp2 de 100 GiB com saldo de crédito vazio tem uma performance basal de 300 IOPS e um limite de taxa de transferência de 75 MiB/s (300 operações de E/S por segundo * 256 KiB por operação de E/S = 75 MiB/s). Quanto maior o volume, maior a performance basal e mais rapidamente o saldo de crédito é reabastecido.

Para obter mais informações sobre como a IOPS é medida, consulte [Características e monitoramento de E/S \(p. 1459\)](#).

Se você perceber que a performance do seu volume é frequentemente limitada ao nível da linha de base (devido a um saldo de crédito de E/S vazio), mude para um volume de gp3.

Para obter informações sobre como usar as métricas e os alarmes do CloudWatch para monitorar seu saldo do bucket de intermitência, consulte [Monitorar o saldo de bucket de intermitência para volumes \(p. 1265\)](#).

Performance de taxa de transferência

A taxa de transferência de um volume gp2 pode ser calculada usando a seguinte fórmula, até o limite de 250 MiB/s de taxa de transferência:

```
Throughput in MiB/s = ((Volume size in GiB) × (IOPS per GiB) × (I/O size in KiB))
```

Supondo que V = tamanho do volume, I = tamanho de entrada/saída e R = taxa de entrada/saída T= taxa de transferência, isso pode ser simplificado em:

```
T = VIR
```

O menor tamanho de volume que atinge a taxa de transferência máxima é determinado por:

$$\begin{aligned} V &= \frac{T}{I \cdot R} \\ &= \frac{250 \text{ MiB/s}}{(256 \text{ KiB})(3 \text{ IOPS/GiB})} \\ &= \frac{[(250)(2^{20})(\text{Bytes})]/\text{s}}{(256)(2^{10})(\text{Bytes})([3 \text{ IOP/s}]/[(2^{30})(\text{Bytes})])} \\ &= \frac{(250)(2^{20})(2^{30})(\text{Bytes})}{(256)(2^{10})(3)} \\ &= 357,913,941,333 \text{ Bytes} \\ &= 333\# \text{ GiB (334 GiB in practice because volumes are provisioned in whole gibibytes)} \end{aligned}$$

Volumes de Provisioned IOPS SSD

Os volumes SSD de IOPS provisionadas (io1 e io2) são criados para atender às necessidades de workloads com uso intensivo de E/S, especialmente workloads de bancos de dados, que são sensíveis a performance e consistência de armazenamento. Os volumes SSD de IOPS provisionadas usam uma taxa de IOPS consistente, que você especifica ao criar o volume, e o Amazon EBS fornece a performance provisionada em 99,9% do tempo.

Volumes io1 são criados para fornecer durabilidade de volume de 99,8 a 99,9% com uma taxa anual de falhas (AFR) de até 0,2%, o que significa no máximo duas falhas de volume por 1.000 volumes em execução durante um período de um ano. Volumes io2 são criados para fornecer 99,999% de durabilidade de volume com uma AFR de até 0,001%, o que significa uma única falha de volume por 100.000 volumes em execução durante um período de um ano.

Os volumes SSD de IOPS provisionadas **io1** e **io2** estão disponíveis para todos os tipos de instância do Amazon EC2. Volumes **io2** de SSD de IOPS provisionadas anexados a instâncias R5b são executados no EBS Block Express. Para obter mais informações, consulte [Volumes io2 Block Express](#).

Considerações para volumes **io2**

- Lembre-se do seguinte ao executar instâncias com volumes **io2**:
 - Se você iniciar uma instância R5b com um volume **io2**, o volume será executado automaticamente no [Block express \(p. 1256\)](#), qualquer que seja o tamanho do volume e da IOPS.
 - Não é possível iniciar um tipo de instância que não seja compatível com o [Block Express \(p. 1256\)](#) com um volume **io2** que tem tamanho superior a 16 TiB ou IOPS superior a 64.000.
 - Não é possível iniciar uma instância R5b com um volume **io2** criptografado que tem tamanho superior a 16 TiB ou IOPS superior a 64.000 de uma AMI não criptografada ou de uma AMI criptografada compartilhada. Nesse caso, você deve primeiro criar uma AMI criptografada em sua conta e depois usar essa AMI para iniciar a instância.
- Lembre-se do seguinte ao criar volumes **io2**:
 - Se você criar um volume **io2** com tamanho superior a 16 TiB ou IOPS superior a 64.000 em uma região que oferece suporte ao [Block Express \(p. 1256\)](#), o volume será executado automaticamente no Block Express.
 - Não é possível criar um volume **io2** com tamanho superior a 16 TiB ou IOPS superior a 64.000 em uma região que não oferece suporte ao [Block Express \(p. 1256\)](#).
 - Se você criar um volume **io2** com tamanho igual ou inferior a 16 TiB ou IOPS igual ou inferior a 64.000 em uma região que oferece suporte ao [Block Express \(p. 1256\)](#), o volume não será executado automaticamente no Block Express.
 - Não é possível iniciar um volume **io2** criptografado que tem tamanho superior a 16 TiB ou IOPS superior a 64.000 de um snapshot não criptografado ou de um snapshot criptografado compartilhado. Nesse caso, você deve primeiro criar um snapshot criptografado em sua conta e depois usar esse snapshot para criar o volume.
- Lembre-se do seguinte ao anexar volumes **io2** a instâncias:
 - Se você anexar um volume **io2** a uma instância R5b, o volume será executado automaticamente no [Block Express \(p. 1256\)](#). Pode levar até 48 horas para otimizar o volume do Block Express. Durante esse tempo, o volume fornece latência **io2**. Depois de otimizado, o volume fornece a latência abaixo de milissegundos compatível com o Block Express.
 - Não é possível anexar um volume **io2** que tem tamanho superior a 16 TiB ou IOPS superior a 64.000 a uma tipo de instância que não seja compatível com o [Block Express \(p. 1256\)](#).
 - Se você desvincular um volume **io2** com tamanho igual ou inferior a 16 TiB e IOPS igual ou inferior a 64.000 de uma instância R5b e anexá-la a um tipo de instância que é compatível com o [Block Express \(p. 1256\)](#), o volume não será mais executado no Block Express e fornecerá latência **io2**.
- Lembre-se do seguinte ao modificar volumes **io2**:
 - Não é possível modificar um volume **io2** e aumentar seu tamanho além de 16 TiB ou suas IOPS além de 64.000 enquanto ele está anexado a um tipo de instância que não é compatível com o [Block Express \(p. 1256\)](#).
 - Não é possível modificar o tamanho ou as IOPS provisionadas de um volume **io2** anexado a uma instância R5b.

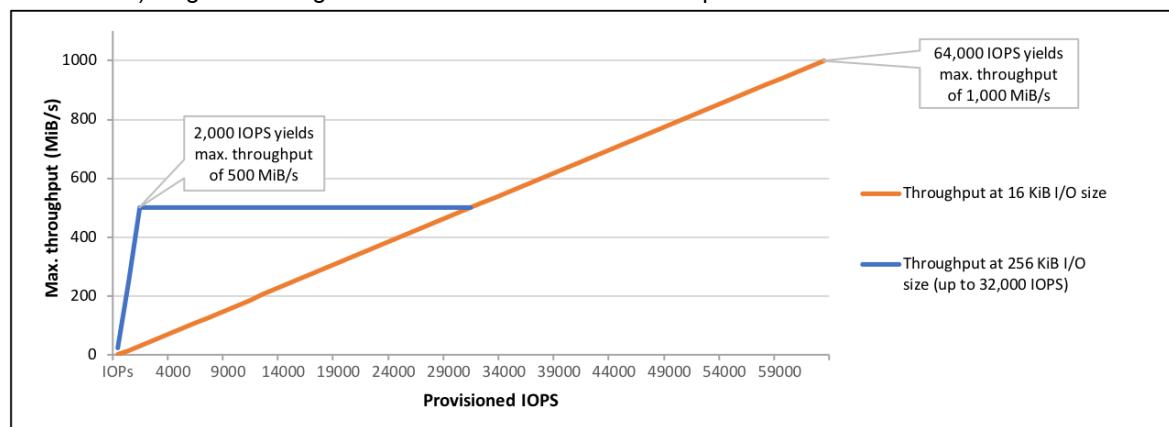
Performance

Os volumes de Provisioned IOPS SSD podem variar de tamanho de 4 GiB até 16 TiB, e você pode provisionar de 100 até 64.000 IOPS por volume. Você pode alcançar somente até 64.000 IOPS em [Instâncias criadas no Sistema Nitro \(p. 154\)](#). Em outras famílias de instâncias, você pode obter uma performance de até 32.000 IOPS. A proporção máxima de IOPS provisionadas para o tamanho do volume solicitado (em GiB) é de 50:1 para volumes **io1** e de 500:1 para volumes **io2**. Por exemplo, um volume de **io1** de 100 GiB pode ser provisionado com até 5.000 IOPS, enquanto um volume de **io2** de 100 GiB

pode ser provisionado com até 50.000 IOPS. Em um tipo de instância compatível, os seguintes tamanhos de volume permitem o provisionamento até o máximo de 64.000 IOPS:

- **io1** volume de 1.280 GiB ou superior ($50 \times 1.280 \text{ GiB} = 64.000 \text{ IOPS}$)
- **io2** Tamanho de volume de 128 GiB ou superior ($500 \times 128 \text{ GiB} = 64.000 \text{ IOPS}$)

Os volumes de Provisioned IOPS SSD provisionados com até 32.000 IOPS oferecem suporte a um tamanho máximo de E/S de 256 KiB e produzem até 500 MiB/s de taxa de transferência. Com o tamanho de E/S máximo, o pico da taxa de transferência é de 2.000 IOPS. Volumes provisionados com mais de 32.000 IOPS (até o máximo de 64.000 IOPS) geram um aumento linear na taxa de transferência a uma taxa de 16 KiB por IOPS provisionadas. Por exemplo, um volume provisionado com 48.000 IOPS pode suportar até 750 MiB/s de taxa de transferência (16 KiB por IOPS provisionadas \times 48.000 IOPS provisionadas = 750 MiB/s). Para alcançar a taxa de transferência máxima de 1.000 MiB/s, deve ser provisionado um volume com 64.000 IOPS (16 KiB por IOPS provisionadas \times 64.000 IOPS provisionadas = 1.000 MiB/s). O gráfico a seguir ilustra essas características de performance:



Sua experiência de latência por E/S depende das IOPS provisionadas e do seu perfil de workload. Para obter a melhor experiência de latência de E/S, certifique-se de provisionar IOPS para atender ao perfil de E/S da sua workload.

Volumes **io2** do Block Express

Note

Os volumes **io2** do Block Express são compatíveis apenas com instâncias R5b.

Os volumes **io2** EBS Block Express é a próxima geração de arquitetura de servidor de armazenamento do Amazon EBS. Ele foi construído com o objetivo de atender aos requisitos de performance das aplicações com uso intensivo de E/S mais exigentes que são executados em instâncias do Amazon EC2 baseadas em Nitro.

A arquitetura Block Express aumenta a performance e a escala. Os servidores Block Express se comunicam com instâncias baseadas em Nitro usando o protocolo de rede Scalable Reliable Datagram (SRD). Essa interface é implementada no Nitro Card dedicado à função de E/S do Amazon EBS no hardware de host da instância. Ela minimiza o atraso de E/S e a variação da latência (tremulação de rede), o que proporciona uma performance mais rápida e consistente para suas aplicações. Para obter mais informações, consulte [Volumes **io2** Block Express](#).

Os volumes **io2** Block Express são adequados para workloads que se beneficiam de um único volume que fornece latência abaixo de um milissegundo e é compatível com IOPS mais altas, maior taxa de transferência e capacidade maior do que volumes **io2**.

Os volumes **io2** do Block Express oferecem suporte aos mesmos recursos que os volumes **io2**, inclusive de operações Multi-Attach, Elastic Volume e criptografia.

Tópicos

- [Considerations \(p. 1257\)](#)
- [Performance \(p. 1257\)](#)
- [Quotas \(p. 1257\)](#)
- [Definição de preço e faturamento \(p. 1258\)](#)

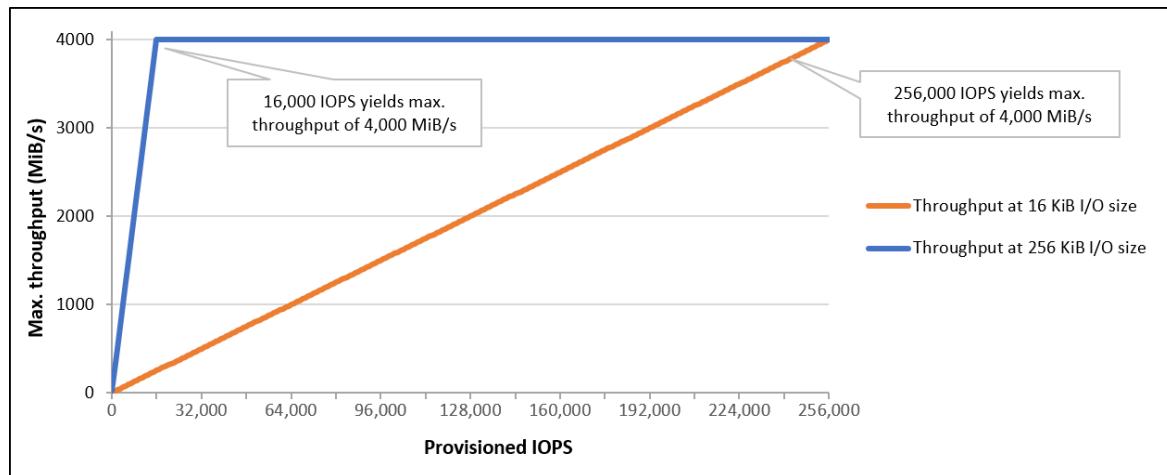
Considerations

- Atualmente, os volumes io2 Block Express são compatíveis apenas com instâncias R5b.
- Os volumes io2 do Block Express estão disponíveis atualmente em todas as regiões onde as instâncias R5b estão disponíveis, inclusive us-east-1, us-east-2, us-west-2, ap-southeast-1, ap-northeast-1 e eu-central-1. A disponibilidade da instância R5b pode variar de acordo com a zona de disponibilidade. Para obter mais informações sobre a disponibilidade do R5b, consulte [Localizar um tipo de instância do Amazon EC2](#).
- Os volumes io2 do Block Express não são compatíveis com a restauração rápida de snapshots. Recomendamos inicializar esses volumes para garantir que eles forneçam performance total. Para obter mais informações, consulte [Inicializar volumes de Amazon EBS \(p. 1463\)](#).

Performance

Com volumes io2 Block Express, é possível provisionar volumes com:

- Latência média de abaixo de milissegundo
- Capacidade de armazenamento de até 64 TiB (65.536 GiB)
- IOPS provisionadas de até 256.000, com uma relação IOPS:GiB de 1.000:1. As IOPS máximas podem ser provisionadas com volumes de 256 GiB de tamanho e maiores ($1.000 \text{ IOPS} \times 256 \text{ GiB} = 256.000 \text{ IOPS}$).
- Taxa de transferência de volume de até 4.000 MiB/s. A taxa de transferência é dimensionada proporcionalmente até 0,256 MiB/s por IOPS provisionadas. A taxa de transferência máxima pode ser alcançada em 16.000 IOPS ou superior.



Quotas

Os volumes io2 Block Express aderem às mesmas cotas de serviço que os volumes io2. Para obter mais informações, consulte [cotas de Amazon EBS](#).

Definição de preço e faturamento

Os volumes io2 e io2 Block Express são cobrados com a mesma taxa. Para obter mais informações, consulte [Definição de preço do Amazon EBS](#).

Os relatórios de uso não fazem distinção entre volumes io2 Block Express e io2. Recomendamos que você use tags para ajudar a identificar os custos associados aos volumes io2 Block Express.

Volumes HDD otimizados para taxa de transferência

Os volumes HDD otimizados para taxa de transferência (st1) fornecem armazenamento magnético de baixo custo que define a performance em termos de taxa de transferência, não IOPS. Esse tipo de volume é ideal para workloads grandes e sequenciais, como Amazon EMR, ETL, datas warehouses e processamento de logs. Não há compatibilidade com volumes de st1 inicializáveis.

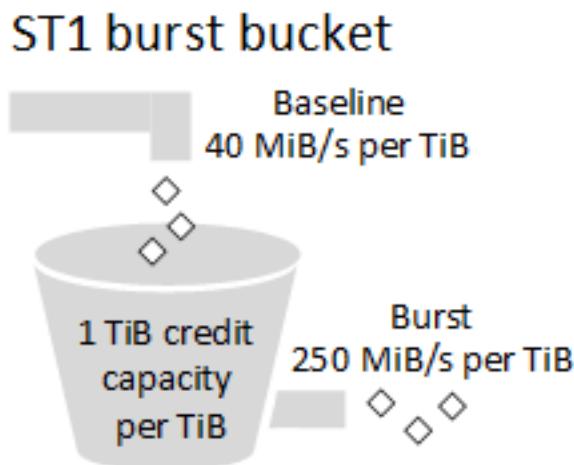
Os volumes HDD otimizados para taxa de transferência (st1), embora semelhantes aos volumes HDD a frio (sc1), são projetados para serem compatíveis com dados acessados com frequência.

Esse tipo de volume é otimizado para workloads que envolvem E/S sequencial e grande, e recomendamos que clientes com workloads executando E/S pequena e aleatória usem gp2. Para obter mais informações, consulte [Ineficiência de pequenas leituras/escritas no HDD \(p. 1265\)](#).

Créditos de taxa de transferência e performance de intermitência

Como o gp2, o st1 usa um modelo de bucket de intermitência para performance. O tamanho do volume determina a taxa de transferência da linha de base do seu volume, que é a taxa na qual o volume acumula créditos de taxa de transferência. O tamanho do volume também determina a taxa de transferência de intermitência do seu volume, que é a taxa em que você pode gastar créditos quando estiverem disponíveis. Os volumes maiores têm taxa de transferência basal e de intermitência mais altos. Quanto mais créditos seu volume tiver, ele será capaz de acionar E/S da unidade em nível de intermitência por mais tempo.

O diagrama a seguir mostra comportamento do bucket de intermitência para st1.



Sujeito a taxa de transferência e limites de crédito de taxa de transferência, a taxa de transferência disponível de um volume st1 é expressada pela seguinte fórmula:

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

Para um volume de st1 de 1-TiB, a taxa de transferência de intermitência está limitada a 250 MiB/s, o bucket se enche com créditos a 40 MiB/s e pode suportar até 1 TiB equivalente em créditos.

Os volumes maiores expandem esses limites de modo linear, com uma taxa de transferência máxima de 500 MiB/s. Depois que o bucket se esgota, a taxa de transferência é limitada à taxa de base de 40 MiB/s por TiB.

Os tamanhos dos volume variando de 0,125 a 16 TiB, a taxa de transferência basal varia de 5 MiB/s até um máximo de 500 MiB/s, que é acessado a 12.5 TiB, da seguinte forma:

$$\frac{40 \text{ MiB/s}}{12.5 \text{ TiB}} = 500 \text{ MiB/s}$$

1 TiB

A taxa de transferência varia de 31 MiB/s a um limite de 500 MiB/s, que é alcançado em 2 TiB, da seguinte forma:

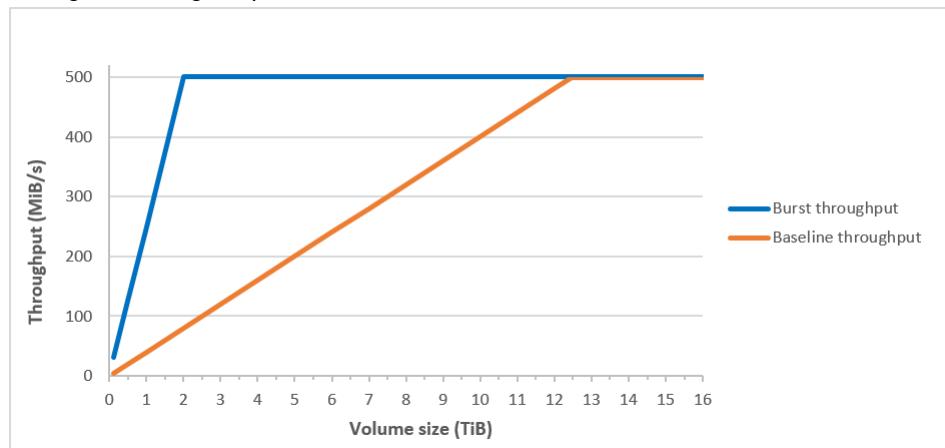
$$\frac{250 \text{ MiB/s}}{2 \text{ TiB}} = 500 \text{ MiB/s}$$

1 TiB

A tabela a seguir apresenta a gama completa de valores de taxa de transferência e intermitência para st1:

Tamanho do volume (TiB)	Taxa de transferência de base ST1 (MiB/s)	Taxa de transferência de intermitência do ST1 (MiB/s)
0,125	5	31
0,5	20	125
1	40	250
2	80	500
3	120	500
4	160	500
5	200	500
6	240	500
7	280	500
8	320	500
9	360	500
10	400	500
11	440	500
12	480	500
12,5	500	500
13	500	500
14	500	500
15	500	500
16	500	500

O diagrama a seguir apresenta os valores da tabela:



Note

Quando você cria um snapshot de um volume HDD otimizado para taxa de transferência (st1), a performance poderá cair até o valor básico do volume enquanto o snapshot estiver em andamento.

Para obter informações sobre como usar as métricas e os alarmes do CloudWatch para monitorar seu saldo do bucket de intermitência, consulte [Monitorar o saldo de bucket de intermitência para volumes \(p. 1265\)](#).

Volumes HDD a frio

Os volumes HDD a frio (sc1) fornecem armazenamento magnético de baixo custo que define a performance em termos de taxa de transferência, não IOPS. Com um limite menor de taxa de transferência que st1, sc1 é uma boa opção para workloads grandes, sequenciais e de dados frios. Se você precisar acesso infrequente aos dados e estiver em busca de economia de custos, o sc1 fornecerá blocos de armazenamento econômico. Não há compatibilidade com volumes de sc1 inicializáveis.

Os volumes HDD a frio (sc1), embora similares aos volumes HDD otimizados para taxa de transferência (st1), são projetados para serem compatíveis com dados acessados com pouca frequência.

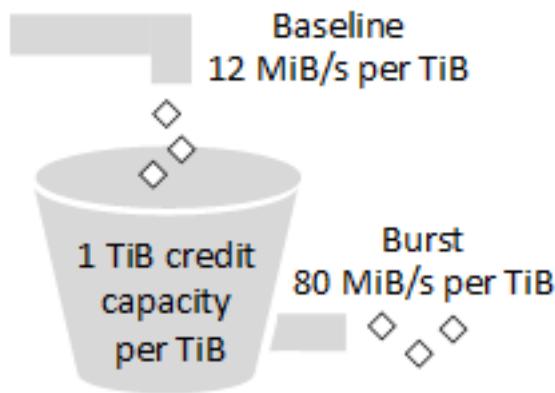
Note

Esse tipo de volume é otimizado para workloads que envolvem E/S sequencial e grande, e recomendamos que clientes com workloads executando E/S pequena e aleatória usem gp2. Para obter mais informações, consulte [Ineficiência de pequenas leituras/escritas no HDD \(p. 1265\)](#).

Créditos de taxa de transferência e performance de intermitência

Como o gp2, o sc1 usa um modelo de bucket de intermitência para performance. O tamanho do volume determina a taxa de transferência da linha de base do seu volume, que é a taxa na qual o volume acumula créditos de taxa de transferência. O tamanho do volume também determina a taxa de transferência de intermitência do seu volume, que é a taxa em que você pode gastar créditos quando estiverem disponíveis. Os volumes maiores têm taxa de transferência basal e de intermitência mais altos. Quanto mais créditos seu volume tiver, ele será capaz de acionar E/S da unidade em nível de intermitência por mais tempo.

SC1 burst bucket



Sujeito a taxa de transferência e limites de crédito de taxa de transferência, a taxa de transferência disponível de um volume sc1 é expressada pela seguinte fórmula:

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

Para um volume de sc1 de 1-TiB, a taxa de transferência de intermitência está limitada a 80 MiB/s, o bucket se enche com créditos a 12 MiB/s e pode suportar até 1 TiB equivalente em créditos.

Os volumes maiores expandem esses limites de modo linear, com uma taxa de transferência máxima de 250 MiB/s. Depois que o bucket se esgota, a taxa de transferência é limitada à taxa de base de 12 MiB/s por TiB.

Os tamanhos dos volume variando de 0,125 a 16 TiB, a taxa de transferência basal varia de 1,5 MiB/s até um máximo de 192 MiB/s, que é acessado a 16 TiB, da seguinte forma:

$$12 \text{ MiB/s} \\ 16 \text{ TiB} \times \frac{12 \text{ MiB/s}}{1 \text{ TiB}} = 192 \text{ MiB/s}$$

A taxa de transferência varia de 10 MiB/s a um limite de 250 MiB/s, que é alcançado em 3.125 TiB, da seguinte forma:

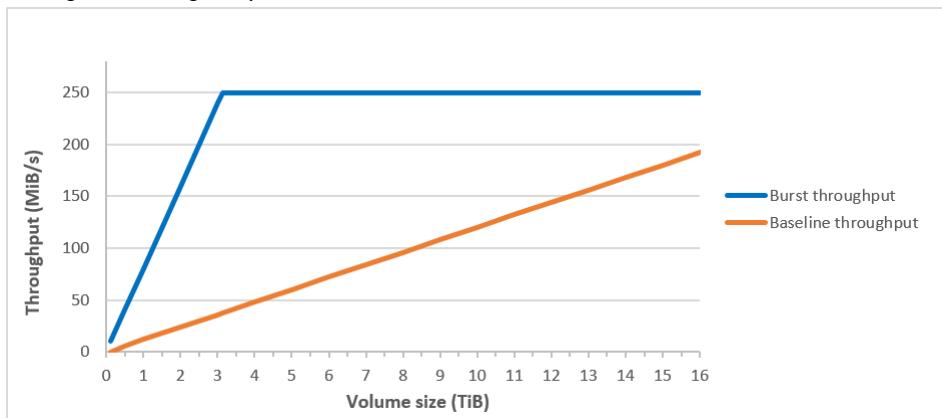
$$80 \text{ MiB/s} \\ 3.125 \text{ TiB} \times \frac{80 \text{ MiB/s}}{1 \text{ TiB}} = 250 \text{ MiB/s}$$

A tabela a seguir apresenta a gama completa de valores de taxa de transferência e intermitência para sc1:

Tamanho do volume (TiB)	Taxa de transferência de base SC1 (MiB/s)	Taxa de transferência de intermitência do SC1 (MiB/s)
0,125	1,5	10
0,5	6	40
1	12	80
2	24	160
3	36	240

Tamanho do volume (TiB)	Taxa de transferência de base SC1 (MiB/s)	Taxa de transferência de intermitência do SC1 (MiB/s)
3.125	37.5	250
4	48	250
5	60	250
6	72	250
7	84	250
8	96	250
9	108	250
10	120	250
11	132	250
12	144	250
13	156	250
14	168	250
15	180	250
16	192	250

O diagrama a seguir apresenta os valores da tabela:



Note

Quando você cria um snapshot de um volume HDD a frio (sc1), a performance poderá cair até o valor básico do volume enquanto o snapshot estiver em andamento.

Para obter informações sobre como usar as métricas e os alarmes do CloudWatch para monitorar seu saldo do bucket de intermitência, consulte [Monitorar o saldo de bucket de intermitência para volumes \(p. 1265\)](#).

Volumes magnéticos

Os volumes magnéticos são baseados em unidades magnéticas e adequados para workloads em que os dados são acessados com pouca frequência, e cenários em que o armazenamento de baixo custo para

pequenos volumes é importante. Esses volumes fornecem aproximadamente 100 IOPS em média, com capacidade de intermitência de até centenas de IOPS, e podem variar em tamanho de 1 GiB de 1 TiB.

Note

O volume magnético é um tipo de volume da geração anterior. Para novas aplicações, recomendamos usar um dos tipos de volume mais novos. Para obter mais informações, consulte [Volumes da geração anterior](#).

Para obter informações sobre como usar as métricas e os alarmes do CloudWatch para monitorar seu saldo do bucket de intermitência, consulte [Monitorar o saldo de bucket de intermitência para volumes \(p. 1265\)](#).

Considerações sobre a performance ao usar volumes de HDD

Para resultados ideais de taxa de transferência usando volumes de HDD, planeje suas workloads com as seguintes considerações em mente.

Comparação entre HDD otimizado para taxa de transferência e HDD a frio

Os tamanhos de bucket st1 e sc1 variam de acordo com o tamanho do volume, e um bucket completo contém tokens suficientes para uma varredura de volume completa. Contudo, volumes de st1 e sc1 maiores demoram mais tempo para varredura do volume ser concluída, em função de limites de taxa de transferência por instância e por volume. Os volumes associados a instâncias menores são limitados à taxa de transferência por instância em vez de aos limites de taxa de transferência de st1 ou sc1.

Tanto st1 quanto sc1 são projetados para consistência de performance de 90% de taxa de transferência de intermitência em 99% do tempo. Períodos não compatíveis são distribuídos com uniformidade aproximada, destinando 99% da taxa de transferência total esperada a cada hora.

Geralmente, os tempos de varredura são expressados por esta fórmula:

$$\frac{\text{Volume size}}{\text{Throughput}} = \frac{\text{Scan time}}{\text{Scan time}}$$

Por exemplo, levando em conta as garantias de consistência da performance e outras otimizações, pode-se esperar que um cliente de st1 com volume de 5-TiB conclua uma varredura de volume completa entre 2,91 e 3,27 horas.

- Tempo de varredura ideal

$$\frac{5 \text{ TiB}}{500 \text{ MiB/s}} = \frac{5 \text{ TiB}}{0.00047684 \text{ TiB/s}} = 10,486 \text{ seconds} = 2.91 \text{ hours}$$

- Tempo máximo de varredura

$$\frac{2.91 \text{ hours}}{(0.90)(0.99)} = 3.27 \text{ hours}$$

--- From expected performance of 90% of burst 99% of the time

Da mesma forma, um cliente de sc1 com volume de 5-TiB pode esperar concluir uma varredura de volume completa em 5,83 a 6,54 horas.

- Tempo de varredura ideal

$\frac{5 \text{ TiB}}{250 \text{ MiB/s}} = \frac{5 \text{ TiB}}{0.000238418 \text{ TiB/s}} = 20972 \text{ seconds} = 5.83 \text{ hours}$
--

- Tempo máximo de varredura

$\frac{5.83 \text{ hours}}{(0.90)(0.99)} = 6.54 \text{ hours}$
--

A tabela a seguir mostra o tempo de varredura ideal de volumes de vários tamanhos, pressupondo buckets cheios e taxa de transferência de instância suficiente.

Tamanho do volume (TiB)	Tempo de varredura de ST1 com intermitênciam (horas) *	Tempo de varredura de SC1 com intermitênciam (horas) *
1	1.17	3.64
2	1.17	3.64
3	1.75	3.64
4	2.33	4.66
5	2.91	5.83
6	3.50	6.99
7	4.08	8.16
8	4.66	9.32
9	5.24	10.49
10	5.83	11.65
11	6.41	12.82
12	6.99	13.98
13	7.57	15.15
14	8.16	16.31
15	8.74	17.48
16	9.32	18.64

* Esses tempos de digitalização pressupõem uma profundidade média de fila (arredondada para o número inteiro mais próximo) de quatro ou mais ao executar 1 MiB de E/S sequencial.

Portanto, se você tiver uma workload orientada para taxa de transferência que precise concluir rapidamente digitalizações (até 500 MiB/s) ou exige várias digitalizações de volume completo por dia, use st1. Se você estiver otimizando para custo, seus dados são acessados com relativa pouca frequência e você não precisar mais de 250 MiB/s de performance da digitalização, use o sc1.

Ineficiência de pequenas leituras/escritas no HDD

O módulo de performance para os volumes `st1` e `sc1` é otimizado para E/Ss sequenciais, favorecendo workloads de alta taxa de transferência, oferecendo performance aceitável em workloads com IOPS e taxa de transferência mistos e desincentivando workloads com E/S pequena e aleatória.

Por exemplo, uma solicitação de E/S de 1 MiB ou menos conta como um 1 de MiB crédito de E/S. Contudo, se as E/Ss forem sequenciais, elas serão fundidas em blocos de 1 MiB de E/S e contarão somente com 1 MiB de crédito de E/S.

Limitações na taxa de transferência por instância

A taxa de transferência dos volumes `st1` e `sc1` sempre é determinado pela menor das seguintes opções:

- Limites de taxa de transferência do volume
- Limites de taxa de transferência da instância

Quanto a todos os volumes da Amazon EBS, recomendamos que você selecione uma instância do EC2 otimizada por EBS adequada para evitar gargalos de rede. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

Monitorar o saldo de bucket de intermitência para volumes

Você pode monitorar o nível do bucket de intermitência para volumes `gp2`, `st1` e `sc1` usando a métrica `BurstBalance` do EBS no Amazon CloudWatch. Essa métrica mostra a porcentagem de créditos de E/S (para `gp2`) ou créditos de taxa de transferência (para `st1` e `sc1`) restantes no bucket de intermitência. Para obter mais informações sobre a métrica `BurstBalance` e outras métricas relacionadas a E/S, consulte [Características e monitoramento de E/S \(p. 1459\)](#). O CloudWatch também permite que você defina um alarme que para notificar a queda do valor de `BurstBalance` para determinado nível. Para obter mais informações, consulte [Criação de alarmes do Amazon CloudWatch](#).

Restrições de tamanho e configuração de um volume do EBS

O tamanho de um volume do Amazon EBS é restrito pela física e pela aritmética do armazenamento de dados em bloco, bem como pelas decisões de implementação dos designers do sistema operacional (SO) e do sistema de arquivos. A AWS impõe limites adicionais sobre o tamanho de volumes para proteger a confiabilidade dos serviços.

As seções a seguir descrevem os fatores mais importantes que limitam o tamanho utilizável de um volume do EBS e oferecem recomendações para configurar seus volumes do EBS.

Tópicos

- [Capacidade de armazenamento \(p. 1265\)](#)
- [Limitações do serviço \(p. 1266\)](#)
- [Esquemas de particionamento \(p. 1266\)](#)
- [Tamanhos de blocos de dados \(p. 1267\)](#)

Capacidade de armazenamento

A tabela a seguir resume as capacidades de armazenamento teóricas e implementadas para a maioria dos sistemas de arquivos usados comumente no Amazon EBS, presumindo um tamanho de bloco de 4.096 bytes.

Esquema de particionamento	Max. de blocos endereçáveis	Tamanho máx. teórico (blocos × tamanho dos blocos)	Tamanho máx. implementado do Ext4*	Tamanho máx. implementado do XFS**	Tamanho máx. implementado do NTFS	Suporte máx. pelo EBS
MBR	2^{32} ³²	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB
GPT	2^{64}	64 ZiB (50 TiB certificados em RHEL7)	1 EiB = 1024 ² TiB (50 TiB certificados em RHEL7)	500 TiB (Certificado na RHEL7)	256 TiB	64 TiB †

* https://ext4.wiki.kernel.org/index.php/Ext4_Howto e <https://access.redhat.com/solutions/1532>

** <https://access.redhat.com/solutions/1532>

† Os volumes io2 Block Express oferecem suporte para até 64 TiB para partições GPT. Para obter mais informações, consulte [Volumes io2 do Block Express \(p. 1256\)](#).

Limitações do serviço

O Amazon EBS abstrai o armazenamento massivamente distribuído de um datacenter em unidades de disco rígido virtuais. Para um sistema operacional instalado em uma instância do EC2, um volume do EBS anexado é exibido como uma unidade de disco rígido virtual contendo setores de disco de 512 bytes. O sistema operacional gerencia a alocação de blocos de dados (ou clusters) nos setores virtuais com os utilitários de gerenciamento de armazenamento. A alocação está em conformidade com um esquema de particionamento de volume, como o registro mestre de inicialização (MBR) ou a tabela de partição do GUID (GPT), e nas capacidades de sistema de arquivos instalado (ext4, NTFS, etc.).

O EBS não considera dados contidos nos setores do disco virtual. Ele garante apenas a integridade dos setores. Isso significa que as ações da AWS e as ações do sistema operacional são completamente independentes umas das outras. Ao selecionar um tamanho de volume, lembre-se dos recursos e dos limites de ambos, como nos seguintes casos:

- Atualmente, o EBS oferece suporte a um tamanho máximo de volume de 64 TiB. Isso significa que você pode criar um volume do EBS de até 64 TiB, mas se o sistema operacional reconhecerá toda essa capacidade dependerá de suas próprias características de projeto e de como o volume está dividido.
- O Amazon EC2 requer volumes de inicialização do Windows para usar o particionamento de MBR. Como abordado em [Esquemas de particionamento \(p. 1266\)](#), isso significa que os volumes de inicialização não podem ser maiores que 2 TiB. Os volumes de dados do Windows não estão sujeitos a esse limite e podem usar o particionamento GPT. Se um volume de inicialização do Windows com 2 TiB ou mais for convertido para usar uma tabela de partição MBR dinâmica, você verá um erro para o volume no Gerenciador de Disco.
- Os volumes de não inicialização do Windows com 2 TiB (2.048 GiB) ou mais devem usar uma tabela de partição GPT para acessar todo o volume. Se um volume do EBS com mais de 2 TiB de tamanho estiver anexado a uma instância do Windows na execução, ele será automaticamente formatado com uma tabela de partição GPT. Se anexar um volume do EBS com mais de 2 TiB de tamanho a uma instância do Windows após a execução, você deverá inicializá-lo com uma tabela GPT manualmente. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#).

Esquemas de particionamento

Entre outros impactos, o esquema de particionamento determina quantos blocos de dados lógicos podem ser endereçados exclusivamente em um único volume. Para obter mais informações, consulte [Tamanhos](#)

de blocos de dados ([p. 1267](#)). Os esquemas comuns de particionamento em uso são registro mestre de inicialização (MBR) e tabela de partição GUID (GPT). As diferenças importantes entre esses esquemas podem ser resumidas da seguinte forma:

MBR

A MBR usa uma estrutura de dados de 32 bits para armazenar endereços de blocos. Isso significa que cada bloco de dados está mapeado com um de 2^{32} números inteiros possíveis. O tamanho endereçável máximo de um volume é determinado pela fórmula a seguir:

$$(2^{32} - 1) \times \text{Block size}$$

O tamanho de bloco para volumes MBR normalmente é limitado a 512 bytes. Portanto:

$$(2^{32} - 1) \times 512 \text{ bytes} = 2 \text{ TiB} - 512 \text{ bytes}$$

As ações alternativas de engenharia para aumentar o limite de 2 TiB para volumes MBR não alcançou a adoção em todo o setor. Portanto, o Linux e o Windows nunca detectam um volume MBR como sendo maior que 2 TiB, mesmo que a AWS mostre seu tamanho como maior.

GPT

A GPT usa uma estrutura de dados de 64 bits para armazenar endereços de blocos. Isso significa que cada bloco de dados está mapeado com um de 2^{64} números inteiros possíveis. O tamanho endereçável máximo de um volume é determinado pela fórmula a seguir:

$$(2^{64} - 1) \times \text{Block size}$$

O tamanho de bloco para volumes GPT normalmente é de 4.096 bytes. Portanto:

$$\begin{aligned} & (2^{64} - 1) \times 4,096 \text{ bytes} \\ &= 2^{64} \times 4,096 \text{ bytes} - 1 \times 4,096 \text{ bytes} \\ &= 2^{64} \times 2^{12} \text{ bytes} - 4,096 \text{ bytes} \\ &= 2^{70} \times 2^6 \text{ bytes} - 4,096 \text{ bytes} \\ &= 64 \text{ ZiB} - 4,096 \text{ bytes} \end{aligned}$$

Os sistemas de computadores do mundo real não são compatíveis com nada próximo desse máximo teórico. O tamanho do sistema de arquivos implementado está limitado atualmente a 50 TiB para ext4 e a 256 TiB para NTFS, ambos excedendo o limite de 16 TiB imposto pela AWS.

Tamanhos de blocos de dados

O armazenamento físico de dados em um disco rígido moderno é controlado pelo endereçamento de blocos lógicos, uma camada de abstração que permite que o sistema operacional leia e grava dados em blocos lógicos sem saber muito sobre o hardware subjacente. O sistema operacional depende do dispositivo de armazenamento para mapear os blocos para seus setores físicos. O EBS anuncia setores de 512 bytes para o sistema operacional, que lê e grava dados no disco usando blocos de dados que são um múltiplo do tamanho do setor.

Atualmente, o tamanho padrão do setor para blocos de dados lógico é de 4.096 bytes (4 KiB). Como determinadas workloads se beneficiam de um tamanho de bloco menor ou maior, os sistemas de arquivos aceitam tamanhos de blocos não padrão que podem ser especificados durante a formatação. Os cenários em que os tamanhos de bloco não padrão devem ser usados estão fora do escopo do tópico, mas a opção de tamanho de bloco tem consequências para a capacidade de armazenamento do volume. A tabela a seguir mostra a capacidade de armazenamento como uma função do tamanho do bloco:

Tamanho de bloco	Tamanho máx. do volume
4 KiB (padrão)	16 TiB
8 KiB	32 TiB
16 KiB	64 TiB
32 KiB	128 TiB
64 KiB (máximo)	256 TiB

O limite imposto pelo EBS no tamanho do volume (16 TiB) atualmente é igual ao tamanho máximo permitido pelos blocos de dados de 4 KiB.

Crie um volume do Amazon EBS.

É possível criar um volume do Amazon EBS e anexá-lo a qualquer instância do EC2 na mesma zona de disponibilidade. Se você criar um volume do EBS criptografado, só poderá anexá-lo a tipos de instância compatíveis. Para obter mais informações, consulte [Tipos de instâncias compatíveis \(p. 1424\)](#).

Se você estiver criando um volume para um cenário de armazenamento de alta performance, use um volume SSD de IOPS provisionadas (`io1` ou `io2`) e associe-o a uma instância com largura de banda suficiente para oferecer suporte a sua aplicação, como uma instância otimizada para EBS. A mesma orientação se aplica a volumes HDD otimizado para taxa de transferência (`st1`) e HDD a frio (`sc1`). Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

Note

Se você criar um volume para uso com uma instância do Windows e ele tiver mais de 2.048 GiB (ou menos de 2.048 GiB, mas for possível aumentá-lo posteriormente), configure o volume para usar tabelas de partição GPT. Para obter mais informações, consulte [Suporte do Windows para discos rígidos maiores que 2 TB..](#)

Os volumes vazios do EBS recebem a performance máxima no momento em que são disponibilizados e não requerem inicialização (antes conhecida como pré-aquecimento). Contudo, os blocos de armazenamento em volumes que foram criados de snapshots devem ser inicializados (extraídos do Amazon S3 e gravados no volume) para você poder acessar o bloco. Essa ação preliminar leva tempo e pode causar um aumento significativo na latência de uma operação de E/S na primeira vez que cada bloco é acessado. A performance do volume é obtida depois que todos os blocos forem obtidos por download e gravados no volume. Para a maioria das aplicações, é aceitável amortizar esse custo ao longo da vida útil do volume. Para evitar essa ocorrência de performance inicial em um ambiente de produção, você pode forçar a inicialização imediata de todo o volume ou habilitar a restauração rápida de snapshots. Para obter mais informações, consulte [Inicializar volumes de Amazon EBS \(p. 1463\)](#).

Important

Se você criar um volume `io2` com tamanho superior a 16 TiB ou IOPS superior a 64,000 em uma região que oferece suporte ao EBS Block Express, o volume será executado automaticamente no `io2` Block Express. Os volumes do Block Express podem ser anexados apenas a instâncias R5b. Para obter mais informações, consulte [Volumes io2 Block Express](#).

Métodos de criação de um volume

- Crie e anexe volumes do EBS ao executar instâncias especificando um mapeamento de dispositivos de blocos. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 419\)](#) e [Mapeamentos de dispositivos de blocos \(p. 1513\)](#).
- Crie um volume do EBS e anexe-o a uma instância em execução. Para obter mais informações, consulte [Criar um volume vazio \(p. 1269\)](#) abaixo.

- Crie um volume do EBS de um snapshot criado anteriormente e anexe-o a uma instância em execução. Para obter mais informações, consulte [Criar um volume a partir de um snapshot \(p. 1270\)](#) abaixo.

Criar um volume vazio

Os volumes vazios recebem sua performance máxima no momento em que estão disponíveis e não exigem inicialização.

Você pode criar um volume EBS vazio usando um dos métodos a seguir.

Console

Para criar um volume EBS vazio usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região em que você gostaria de criar seu volume. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre Regiões, enquanto outros não podem. Para obter mais informações, consulte [Localizações de recursos \(p. 1544\)](#).
3. No painel de navegação, escolha ELASTIC BLOCK STORE, Volumes.
4. Escolha Create Volume (Criar volume).
5. Em Tipo de volume, escolha um tipo de volume. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#).
6. Para Size (Tamanho), informe o tamanho do volume, em GiB. Para obter mais informações, consulte [Restrições de tamanho e configuração de um volume do EBS \(p. 1265\)](#).
7. Para IOPS, informe o número máximo de operações de entrada/saída por segundo (IOPS) ao qual o volume deve oferecer suporte. Você pode especificar IOPS somente para volumes de gp3 io1io2.
8. Para a Throughput (Taxa de transferência), insira a taxa de transferência que o volume deve fornecer, em MiB/s. Você pode especificar a taxa de transferência somente para volumes de gp3.
9. Para Availability Zone (Zona de disponibilidade), escolha a zona de disponibilidade na qual criar o volume. Um volume do EBS deve ser vinculado a uma instância do EC2 que esteja na mesma zona de disponibilidade do volume.
10. (Opcional) Se o tipo de instância oferecer suporte à criptografia do EBS e você quiser criptografar o volume, selecione Encrypt this volume (Criptografar este volume) e escolha uma CMK. Se a criptografia por padrão estiver habilitada nessa região, a criptografia do EBS será habilitada e a CMK padrão para criptografia do EBS será escolhida. Você pode escolher uma CMK diferente da Master Key (Chave mestra) ou colar o ARN completo de qualquer chave que você possa acessar. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).
11. (Opcional) Escolha Create additional tags (Criar tags adicionais) para adicionar tags ao volume. Para cada tag, forneça uma chave e um valor. Para obter mais informações, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).
12. Escolha Create Volume (Criar volume). O volume está pronto para uso quando o status do volume é Disponível.
13. Para usar seu novo volume, anexe-o a uma instância, formate-o e monte-o. Para obter mais informações, consulte [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#).

AWS CLI

Como criar um volume vazio do EBS usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [create-volume](#) (AWS CLI)
- [New-EC2Volume](#) (AWS Tools for Windows PowerShell)

Criar um volume a partir de um snapshot

Os volumes criados de snapshots são carregados lentamente em segundo plano. Isso significa que não há necessidade de esperar que todos os dados sejam transferidos do Amazon S3 para o volume do EBS para que a instância possa começar a acessar um volume anexado e todos os seus dados. Se sua instância acessar dados que ainda não foram carregados, o volume imediatamente baixará os dados solicitados do Amazon S3 e continuará carregando o restante dos dados do volume em segundo plano. A performance do volume é obtida depois que todos os blocos forem obtidos por download e gravados no volume. Para evitar a ocorrência de performance inicial em um ambiente de produção, consulte [Iniciar volumes de Amazon EBS](#) (p. 1463).

Os novos volumes do EBS criados de snapshots criptografados são criptografados automaticamente. Também é possível criptografar um volume rapidamente ao mesmo tempo que o restaura de um snapshot não criptografado. Os volumes criptografados só podem ser anexados a tipos de instâncias que oferecem suporte à criptografia do EBS. Para obter mais informações, consulte [Tipos de instâncias compatíveis](#) (p. 1424).

Você pode criar um volume a partir de um snapshot usando um dos métodos a seguir.

Console

Para restaurar um volume do EBS a partir de um snapshot usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região em que seu snapshot está localizado.

Para usar o snapshot para criar um volume em uma região diferente, copie o snapshot na nova região e use-o para criar um volume nessa região. Para obter mais informações, consulte [Copiar um snapshot do Amazon EBS](#) (p. 1317).

3. No painel de navegação, escolha ELASTIC BLOCK STORE, Volumes.
4. Escolha Create Volume (Criar volume).
5. Em Tipo de volume, escolha um tipo de volume. Para obter mais informações, consulte [Tipos de volume do Amazon EBS](#) (p. 1247).
6. Para Snapshot ID (ID do snapshot), comece a digitar o ID ou a descrição do snapshot do qual está restaurando o volume e selecione-o na lista de opções sugeridas.
7. (Opcional) Selecione Encrypt this volume (Criptografar este volume) para alterar o estado de criptografia do seu volume. Isso será opcional se a [criptografia por padrão](#) (p. 1426) estiver habilitada. Selecione um CMK de Master Key (Chave mestra) para especificar um CMK diferente do CMK padrão para criptografia do EBS.
8. Em Size (Tamanho), verifique se o tamanho padrão do snapshot atende às suas necessidades ou insira o tamanho do volume, em GiB.

Se você especificar um tamanho de volume e um de snapshot, o tamanho deverá ser igual ou maior que o tamanho do snapshot. Quando você seleciona um tipo de volume e um ID de snapshot, os tamanhos mínimo e máximo do volume são mostrados ao lado da lista Size (Tamanho). Para obter mais informações, consulte [Restrições de tamanho e configuração de um volume do EBS](#) (p. 1265).

9. Para IOPS, informe o número máximo de operações de entrada/saída por segundo (IOPS) ao qual o volume deve oferecer suporte. Você pode especificar IOPS somente para volumes de gp3 io1io2.
10. Para a Throughput (Taxa de transferência), insira a taxa de transferência que o volume deve fornecer, em MiB/s. Você pode especificar a taxa de transferência somente para volumes de gp3.

11. Para Availability Zone (Zona de disponibilidade), escolha a zona de disponibilidade na qual criar o volume. Um volume do EBS deve ser vinculado a uma instância do EC2 que esteja na mesma zona de disponibilidade do volume.
12. (Opcional) Escolha Create additional tags (Criar tags adicionais) para adicionar tags ao volume. Para cada tag, forneça uma chave e um valor.
13. Escolha Create Volume (Criar volume).
14. Para usar o novo volume, anexe-o a uma instância e monte-o. Para obter mais informações, consulte [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#).
15. Se tiver criado um volume maior do que o snapshot, você deverá estender o sistema de arquivos no volume para aproveitar o espaço extra. Para obter mais informações, consulte [Volumes elásticos do Amazon EBS \(p. 1409\)](#).

AWS CLI

Para criar um volume do EBS a partir de um snapshot usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [create-volume](#) (AWS CLI)
- [New-EC2Volume](#) (AWS Tools for Windows PowerShell)

Vincular um volume de Amazon EBS a uma instância

Você pode anexar um volume do EBS disponível a uma ou mais de suas instâncias que estejam na mesma zona de disponibilidade que o volume.

Para obter informações sobre como adicionar volumes do EBS à instância na execução, consulte [Mapeamento de dispositivos de blocos de instância \(p. 1519\)](#).

Prerequisites

- Determine quantos volumes você pode associar à sua instância. Para obter mais informações, consulte [Limites de volumes de instância \(p. 1507\)](#).
- Se um volume for criptografado, ele só poderá ser associado a uma instância de suporte Criptografia de Amazon EBS. Para obter mais informações, consulte [Tipos de instâncias compatíveis \(p. 1424\)](#).
- Se um volume tiver um código de produto do AWS Marketplace :
 - O volume só poderá ser associado a uma instância interrompida.
 - Você deve estar inscrito no código do AWS Marketplace que estiver no volume.
 - A configuração (tipo de instância, sistema operacional) da instância deve oferecer suporte ao código AWS Marketplace específico. Por exemplo, você não pode obter um volume de uma instância do Windows e associá-la a uma instância do Linux.
- AWS Marketplace Os códigos de produto do são copiados do volume para a instância.

Important

Se você anexar um volume `io2` a uma instância R5b, o volume sempre será executado no EBS Block Express. No momento, somente instâncias R5b oferecem suporte a volumes `io2` do Block Express. Para obter mais informações, consulte [Volumes `io2` Block Express](#).

Você pode anexar um volume a uma instância usando um dos métodos a seguir.

Console

Para associar um volume do EBS a uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic Block Store, Volumes.
3. Selecione um volume disponível e escolha Actions e Attach Volume.
4. Para Instance, comece a digitar o nome ou ID da instância. Selecione a instância na lista de opções (somente instâncias que estão na mesma Zona de disponibilidade que o volume são exibidas).
5. Para Device, mantenha o nome de dispositivo sugerido ou digite um nome de dispositivo suportado diferente. Para obter mais informações, consulte [Nomes de dispositivos em instâncias do Windows. \(p. 1512\)](#).
6. Escolha Associar.
7. Conecte-se à sua instância e monte o volume. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#).

AWS CLI

Para associar um volume do EBS a uma instância usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [attach-volume \(AWS CLI\)](#)
- [Add-EC2Volume \(AWS Tools for Windows PowerShell\)](#)

Note

Em algumas situações, você pode descobrir que um volume além do volume associado a /dev/xvda ou /dev/sda tornou-se o volume do dispositivo raiz da sua instância. Isso pode acontecer quando você associar o volume do dispositivo raiz de outra instância, ou um volume criado a partir do snapshot de um volume do dispositivo raiz, a uma instância com um volume do dispositivo raiz existente. Para obter mais informações, consulte [Inicialização a partir do volume errado](#).

Disponibilizar um volume do Amazon EBS para uso no Windows

Depois que você associar um volume do Amazon EBS à instância executada no hipervisor Xen, ele será exposto como um dispositivo de blocos e aparecerá como um disco removível no Windows. Você pode formatar o volume com qualquer sistema de arquivos e então montá-lo. Após disponibilizar o volume do EBS para uso, você poderá acessá-lo das mesmas maneiras que acessa qualquer outro volume. Todos os dados gravados nesse sistema de arquivos são gravados no volume do EBS e são transparentes para aplicações que usam o dispositivo.

Em instâncias Nitro, o volume Amazon EBS é exposto como um dispositivo de blocos quando o controlador NVMe verificar o barramento PCI. O disco não aparece como removível. Ao contrário das instâncias baseadas em Xen, há apenas um controlador NVMe por volume do EBS nas instâncias Nitro.

Você pode tirar snapshots do volume do EBS para fins de backup ou para usar como linha de base quando criar outro volume. Para obter mais informações, consulte [Snapshots do Amazon EBS \(p. 1294\)](#).

Você pode obter instruções sobre volumes em uma instância Linux em [Disponibilização de um volume para uso no Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Você pode disponibilizar um volume do EBS para uso por meio do utilitário de gerenciamento de disco e a ferramenta de linha de comando DiskPart.

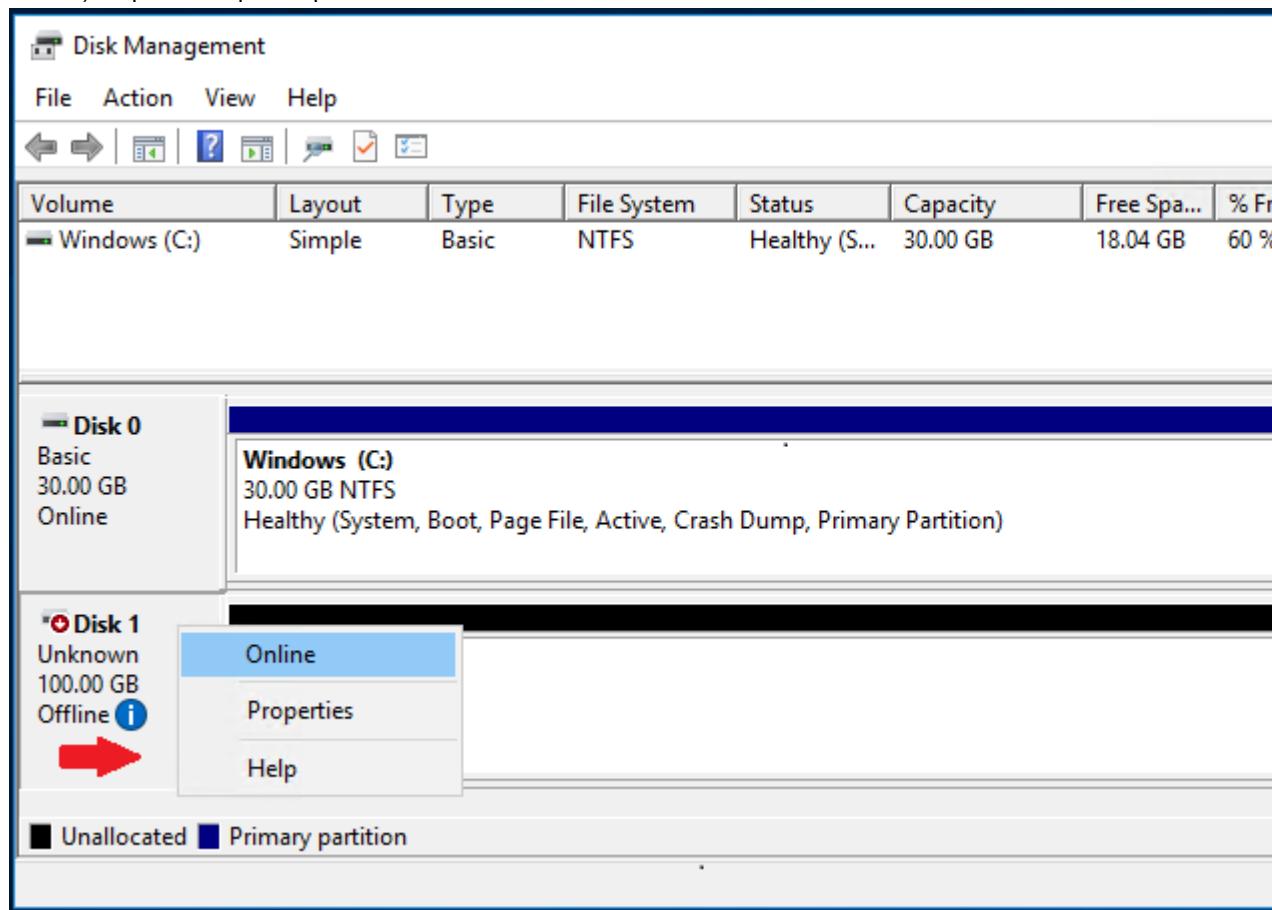
Para disponibilizar um volume do EBS para uso por meio do utilitário de gerenciamento de disco

1. Execute a sessão da sua instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
2. Inicie o utilitário de Gerenciamento de Disco. Na barra de ferramentas, abra o menu de contexto (clique com o botão direito do mouse) no logo do Windows e escolha Disk Management.

Note

No Windows Server 2008, escolha Iniciar, Ferramentas administrativas, Gerenciamento do computador, Disk Management.

3. Traga o volume online. No painel inferior, abra o menu de contexto (clique com o botão direito do mouse) no painel esquerdo para o disco do volume do EBS. Escolha Online.

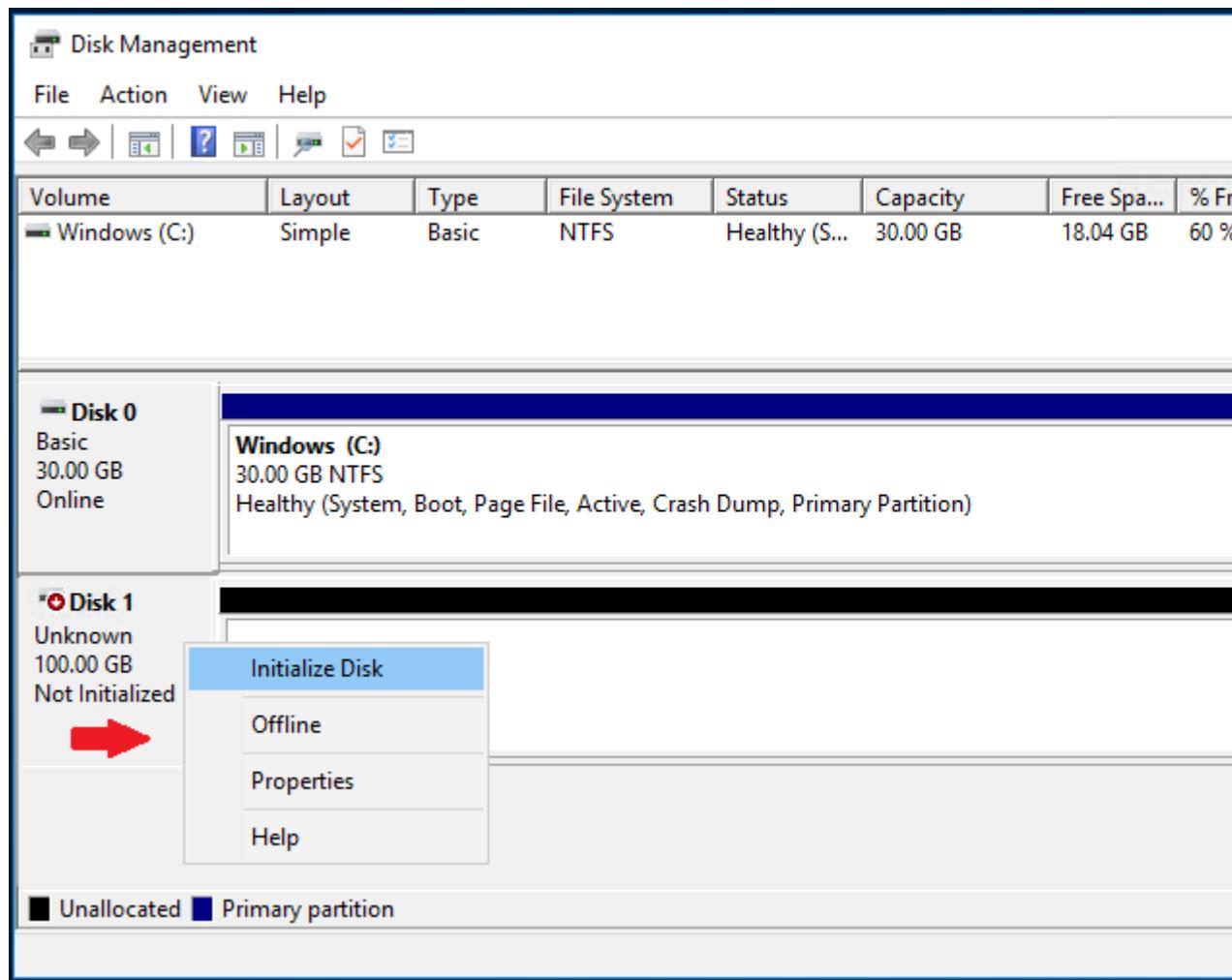


4. (Condisional) Você precisa inicializar o disco antes de usá-lo.

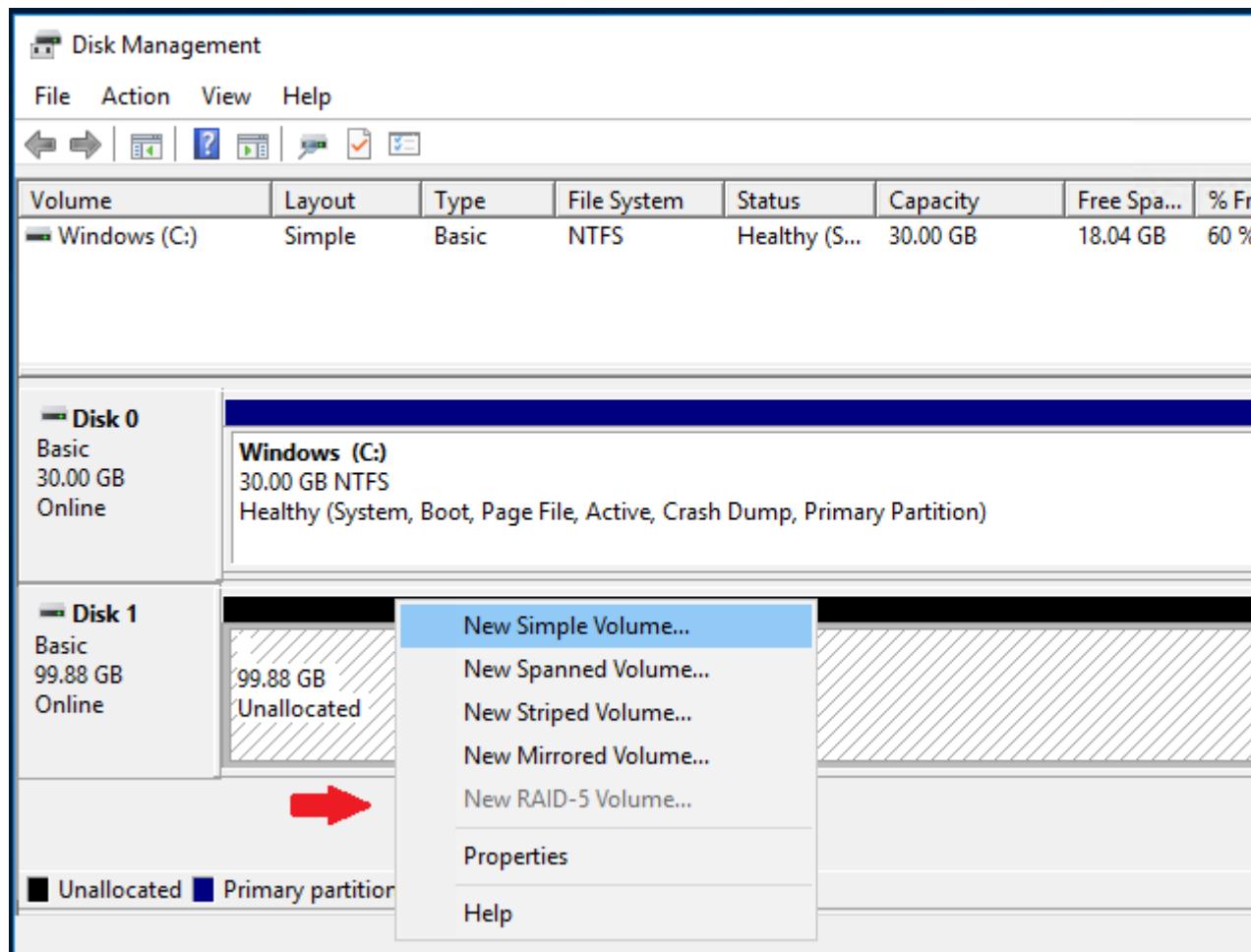
Warning

Se você estiver montando um volume que já tenha dados (por exemplo, um banco de dados públicos ou um volume que você criou a partir de um snapshot), não reformathe o volume. Caso contrário, você excluirá os dados existentes.

Se o disco não for inicializado, inicialize-o da seguinte forma. Abra o menu de contexto (clique com o botão direito do mouse) no painel esquerdo do disco e escolha Disk Management. Na caixa de diálogo Initialize Disk, selecione um estilo de partição e escolha OK.



5. Abra o menu de contexto (clique com o botão direito do mouse) no painel direito do disco e escolha New Simple Volume. Assista todo o assistente.



Para disponibilizar um volume do EBS para uso por meio da ferramenta de linha de comando DiskPart

1. Execute a sessão da sua instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
2. Crie um novo script denominado diskpart.txt.
3. Adicione os seguintes comandos ao arquivo de script e especifique o rótulo do volume e a letra da unidade. Esse script configura o volume para usar a estrutura de partição do registro mestre de inicialização (MBR), formata o volume como um volume NTFS, define o rótulo do volume e atribui a ele uma letra de unidade.

Warning

Se você estiver montando um volume que já tenha dados, não reformato o volume. Caso contrário, excluirá os dados existentes.

```
select disk 1
attributes disk clear readonly
online disk
convert mbr
create partition primary
format quick fs=ntfs label="volume_label"
```

```
assign letter="drive_letter"
```

Para obter mais informações, consulte [Sintaxe e parâmetros da DiskPart](#).

4. Navegue até a pasta na qual o script está localizado e execute o seguinte comando:

```
C:\> diskpart /s diskpart.txt
```

Visualizar informações sobre um volume do Amazon EBS

Você pode visualizar informações descritivas sobre os seus volumes do EBS. Por exemplo, você pode visualizar informações sobre todos os volumes em uma região específica ou visualizar informações detalhadas sobre um único volume, incluindo seu tamanho, tipo de volume, se o volume é criptografado, a chave mestra usada para criptografar o volume e a instância específica à qual o volume está associado.

Você pode obter informações adicionais sobre os seus volumes do EBS, como, por exemplo, o espaço em disco disponível, no sistema operacional da instância.

Visualizar informações de volume

É possível exibir informações sobre um volume usando um dos métodos a seguir.

Console

Para visualizar informações sobre um volume do EBS usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes.
3. (Opcional) Use as opções de filtro no campo de pesquisa para exibir apenas os volumes do seu interesse. Por exemplo, se você souber o ID da instância, escolha Instance ID (ID da instância) no menu do campo de pesquisa e selecione o ID da instância na lista fornecida. Para remover um filtro, selecione-o novamente.
4. Selecione o volume.
5. No painel de detalhes, você pode inspecionar as informações fornecidas sobre o volume. As Informações da anexação mostram o ID de instância à qual este volume está anexado e o nome do dispositivo sob o qual está anexado.
6. (Opcional) Escolha o link Attachment information (Informações da anexação) para visualizar os detalhes adicionais da instância.

Como visualizar os volumes do EBS que estão anexados a uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância.
4. Na guia Storage (Armazenamento), visualize as informações fornecidas sobre dispositivos de bloco e raiz.
5. (Opcional) Escolha um link na coluna Volume ID (ID do volume) para visualizar detalhes adicionais do volume.

AWS CLI

Para visualizar informações sobre um volume do EBS usando a linha de comando

Você pode usar um dos seguintes comandos para visualizar os atributos de volume. Para obter mais informações, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [describe-volumes](#) (AWS CLI)
- [Get-EC2Volume](#) (AWS Tools for Windows PowerShell)

Amazon EC2 Global View

Você pode usar o Amazon EC2 Global View para exibir seus volumes em todas as Regiões para as quais sua conta AWS está habilitada. Para obter mais informações, consulte [Listar e filtrar recursos entre Regiões usando o Amazon EC2 Global View \(p. 1553\)](#).

Estado do volume

O estado do volume descreve a disponibilidade de um volume do Amazon EBS. É possível visualizar o estado do volume na coluna State (Estado), na página Volumes do console, ou usando o comando da AWS CLI [describe-volumes](#).

Os possíveis estados de volume são:

creating

O volume está sendo criado.

available

O volume não está anexado a uma instância.

in-use

O volume está anexado a uma instância.

deleting

O volume está sendo excluído.

deleted

O volume foi excluído.

error

Houve falha no hardware subjacente relacionado ao volume do EBS e os dados associados ao volume são irrecuperáveis. Para obter informações sobre como restaurar o volume ou recuperar os dados no volume, consulte [Meu volume do EBS tem um status de “erro”](#).

Visualizar métricas de volume

Você pode obter informações adicionais sobre seus volumes do EBS no Amazon CloudWatch. Para obter mais informações, consulte [Métricas do Amazon CloudWatch para o Amazon EBS \(p. 1472\)](#).

Visualizar espaço livre em disco

Você pode obter informações adicionais sobre os seus volumes do EBS, como, por exemplo, o espaço em disco disponível, no sistema operacional Windows da instância. Por exemplo, você pode visualizar o espaço em disco disponível abrindo o Explorador de Arquivos e selecionando This PC (Este PC).

Você também pode visualizar o espaço em disco disponível usando o comando `dir` a seguir e examinando a última linha da saída:

```
C:\> dir C:  
Volume in drive C has no label.  
Volume Serial Number is 68C3-8081
```

```
Directory of C:\

03/25/2018  02:10 AM    <DIR>      .
03/25/2018  02:10 AM    <DIR>      ..
03/25/2018  03:47 AM    <DIR>      Contacts
03/25/2018  03:47 AM    <DIR>      Desktop
03/25/2018  03:47 AM    <DIR>      Documents
03/25/2018  03:47 AM    <DIR>      Downloads
03/25/2018  03:47 AM    <DIR>      Favorites
03/25/2018  03:47 AM    <DIR>      Links
03/25/2018  03:47 AM    <DIR>      Music
03/25/2018  03:47 AM    <DIR>      Pictures
03/25/2018  03:47 AM    <DIR>      Saved Games
03/25/2018  03:47 AM    <DIR>      Searches
03/25/2018  03:47 AM    <DIR>      Videos
          0 File(s)        0 bytes
       13 Dir(s)   18,113,662,976 bytes free
```

Você também pode visualizar o espaço em disco disponível usando o seguinte comando `fsutil`:

```
C:\> fsutil volume diskfree C:
Total # of free bytes      : 18113204224
Total # of bytes           : 32210153472
Total # of avail free bytes : 18113204224
```

Para obter informações sobre como visualizar o espaço livre em disco em uma instância do Linux, consulte [View free disk space \(Ver espaço livre em disco\)](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Substituir um volume do Amazon EBS

Os snapshots do Amazon EBS são a ferramenta de backup preferida do Amazon EC2 devido à sua velocidade, conveniência e custo. Ao criar um volume de um snapshot, você recria o estado dele para um ponto específico no passado com todos os dados intactos. Ao anexar um volume criado de um snapshot a uma instância, é possível duplicar os dados entre regiões, criar ambientes de teste, substituir um volume de produção danificado ou corrompido em sua totalidade ou recuperar arquivos e diretórios específicos e transferi-los para outro volume anexado. Para obter mais informações, consulte [Snapshots do Amazon EBS \(p. 1294\)](#).

O procedimento para substituir um volume difere dependendo se o volume for o volume raiz ou um volume de dados.

Tópicos

- [Substituir um volume raiz \(p. 1278\)](#)
- [Substituir um volume de dados \(p. 1281\)](#)

Substituir um volume raiz

Amazon EC2 permite substituir o volume raiz do EBS por uma instância em execução sem interrompê-la. Você pode restaurar o volume raiz de uma instância para seu estado de inicialização ou para um snapshot específico. Isso permite que você corrija problemas, como corrupção de volume raiz ou erros de configuração de rede do sistema operacional convidado, mantendo o seguinte:

- Dados armazenados em volumes de armazenamento de instâncias — Os volumes de armazenamento de instâncias permanecem anexados à instância após a substituição do volume raiz.
- Configuração de rede — Todas as interfaces de rede permanecem conectadas à instância e mantêm seus endereços IP, identificadores e IDs de anexo. Quando a instância fica disponível, todo o tráfego de

rede pendente é liberado. Além disso, a instância permanece no mesmo host físico, portanto, mantém seus endereços IP públicos e privados e o nome DNS.

- Políticas do IAM — IAM os perfis e as políticas (como políticas baseadas em tags) associados à instância são mantidos e impostos.

Quando você substitui o volume raiz de uma instância, um novo volume é restaurado para o estado de inicialização do volume original ou usando um snapshot específico. O volume original é separado da instância e o novo volume é anexado à instância em seu lugar. O volume original não é excluído automaticamente. Se você não precisar mais dele, poderá excluí-lo manualmente após a conclusão da tarefa de substituição do volume raiz. Para obter mais informações sobre os estados da tarefa de substituição do volume raiz, consulte [Exibir tarefas de substituição do volume raiz \(p. 1280\)](#).

Tópicos

- [Considerations \(p. 252\)](#)
- [Substituir um volume raiz \(p. 1279\)](#)
- [Exibir tarefas de substituição do volume raiz \(p. 1280\)](#)

Considerations

- A instância é reinicializada automaticamente quando o volume raiz é substituído. O conteúdo da memória (RAM) é apagado durante a reinicialização.
- Não é possível substituir o volume raiz se ele for um volume de armazenamento de instâncias.
- Não é possível substituir o volume raiz para instâncias metálicas.
- Só é possível usar snapshots que pertencem à mesma linhagem que o volume raiz atual da instância. Não é possível usar cópias de snapshots criadas de snapshots que foram tirados do volume raiz. Além disso, depois de concluir corretamente uma tarefa de substituição de volume raiz, os snapshots tirados do volume raiz anterior não podem ser usados para criar uma tarefa de substituição de volume raiz para o novo volume.

Substituir um volume raiz

Quando você substitui o volume raiz de uma instância, você pode optar por restaurar o volume para seu estado de inicialização inicial ou por restaurar o volume para um snapshot específico. Se você optar por restaurar o volume para um snapshot específico, selecione um snapshot que tenha sido retirado desse volume raiz. Se você optar por restaurar o volume raiz para seu estado de inicialização inicial, o volume raiz será restaurado a partir do snapshot que foi usado para criar o volume.

Você pode substituir o volume raiz de uma instância usando um dos métodos a seguir. Se você usar o console do Amazon EC2, observe que a substituição do volume raiz só estará disponível no novo console.

Amazon EC2 console

Para substituir o volume raiz

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que será substituída pelo volume raiz e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas) e Replace root volume (Substituir volume raiz).
4. Na tela Replace root volume (Substituir volume raiz), siga um destes procedimentos:
 - Para restaurar o volume raiz da instância para seu estado de inicialização inicial, escolha Create replacement task (Criar tarefa de substituição) sem selecionar um snapshot.

- Para restaurar o volume raiz da instância em um snapshot específico, selecione o snapshot a ser usado e escolha Create replacement task (Criar tarefa de substituição).

AWS CLI

Para restaurar o volume raiz para o estado de inicialização inicial

Use o comando `create-replace-root-volume-task`. Especifique o ID da instância para a qual substituir o volume raiz e omitir o `--snapshot-id` parâmetro.

```
$ aws ec2 create-replace-root-volume-task --instance-id instance_id
```

Por exemplo:

```
$ aws ec2 create-replace-root-volume-task --instance-id i-1234567890abcdef0
```

Para restaurar o volume raiz em um snapshot específico

Use o comando `create-replace-root-volume-task`. Especifique o ID da instância para a qual substituir o volume raiz e o ID do snapshot a ser usado.

```
$ aws ec2 create-replace-root-volume-task --instance-id instance_id --snapshot-id snapshot_id
```

Por exemplo:

```
$ aws ec2 create-replace-root-volume-task --instance-id i-1234567890abcdef0 --snapshot-id snap-9876543210abcdef0
```

Exibir tarefas de substituição do volume raiz

Depois de iniciar uma tarefa de substituição de volume raiz, a tarefa insere os seguintes estados:

- `pending` — o volume de substituição está sendo criado.
- `in-progress` — o volume original está sendo destacado e o volume de substituição está sendo anexado.
- `succeeded` — o volume de substituição foi anexado com êxito à instância e a instância está disponível.
- `failing` — a tarefa de substituição está em processo de falha.
- `failed` — a tarefa de substituição falhou, mas o volume raiz original ainda está anexado.
- `failing-detached` — a tarefa de substituição está em processo de falha. A instância pode não ter volume raiz anexado.
- `failed-detached` — a tarefa de substituição falhou e a instância não tem volume raiz anexado.

Você pode exibir as tarefas de substituição do volume raiz de uma instância usando um dos seguintes métodos.

Amazon EC2 console

Para exibir as tarefas de substituição do volume raiz

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).

3. Selecione a instância para a qual deseja exibir as tarefas de substituição do volume raiz e escolha a guia Storage (Armazenamento).
4. Na guia Storage (Armazenamento), expanda Recent root volume replacement tasks (Tarefas recentes de substituição de volume raiz).

AWS CLI

Para exibir o status de uma tarefa de substituição de volume raiz

Use o comando [describe-replace-root-volume-tasks](#) e especifique os IDs das tarefas de substituição do volume raiz a serem visualizadas.

```
$ aws ec2 describe-replace-root-volume-tasks --replace-root-volume-task-ids task_id_1 task_id_2
```

Por exemplo:

```
$ aws ec2 describe-replace-root-volume-tasks --replace-root-volume-task-ids replacevol-1234567890abcdef0
```

```
{
  "ReplaceRootVolumeTasks": [
    {
      "ReplaceRootVolumeTaskId": "replacevol-1234567890abcdef0",
      "InstanceId": "i-1234567890abcdef0",
      "TaskState": "succeeded",
      "StartTime": "2020-11-06 13:09:54.0",
      "CompleteTime": "2020-11-06 13:10:14.0"
    }
  ]
}
```

Como alternativa, especifique o filtro `instance-id` para filtrar os resultados por instância.

```
$ aws ec2 describe-replace-root-volume-tasks --filters Name=instance-id,Values=instance_id
```

Por exemplo:

```
$ aws ec2 describe-replace-root-volume-tasks --filters Name=instance-id,Values=i-1234567890abcdef0
```

Substituir um volume de dados

Use o procedimento a seguir para substituir um volume de dados (não raiz) por outro volume criado de um snapshot anterior desse volume. É necessário desanexar o volume atual e anexar o novo volume.

Observe que os volumes do EBS só podem ser anexados a instâncias do EC2 na mesma zona de disponibilidade.

Use o método a seguir.

Console

Para substituir um volume de dados

1. Crie um volume usando o snapshot e anote o ID do novo volume. Para obter mais informações, consulte [Criar um volume a partir de um snapshot \(p. 1270\)](#).
2. Na página de volumes, marque a caixa de seleção do volume a ser substituído. Na guia Description (Descrição), localize as informações da associação e anote o nome do dispositivo do volume (por exemplo, /dev/sda1) e o ID da instância.
3. Com o volume ainda selecionado, escolha Ações, Desanexar volume. Quando a confirmação for solicitada, escolha Yes, Detach (Sim, separar). Desmarque a caixa de seleção desse volume.
4. Marque a caixa de seleção do novo volume que você criou na etapa 1. Escolha Ações, Anexar volume. Insira o ID da instância e o nome do dispositivo que você anotou na etapa 2 e selecione Anexar.
5. Conecte-se à sua instância e monte o volume. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#).

Monitorar o status de seus volumes

A Amazon Web Services (AWS) fornece automaticamente dados que você pode usar para monitorar seus volumes do Amazon Elastic Block Store (Amazon EBS).

Tópicos

- [Verificações de status do volume do EBS \(p. 1282\)](#)
- [Eventos de volume do EBS \(p. 1284\)](#)
- [Trabalhar com um volume danificado \(p. 1286\)](#)
- [Trabalhar com o atributo de volume de E/S habilitada automaticamente \(p. 1288\)](#)

Para obter informações adicionais sobre o monitoramento, consulte [Métricas do Amazon CloudWatch para o Amazon EBS \(p. 1472\)](#) e [Amazon CloudWatch Events para Amazon EBS \(p. 1479\)](#).

Verificações de status do volume do EBS

As verificações de status de volume permitem que você compreenda, rastreie e gerencie melhor as inconsistências potenciais nos dados em um volume do Amazon EBS. Elas foram desenvolvidas para fornecer as informações necessárias para determinar se os volumes do Amazon EBS estão danificados e para ajudar a controlar como um volume potencialmente inconsistente é manuseado.

As verificações de status de volume são os testes automatizados que executam a cada cinco minutos e retornam um status de êxito ou de falha. Se todas as verificações tiverem êxito, o status do volume será `ok`. Se houve falha em uma verificação, o status do volume será `impaired`. Se o status for `insufficient-data`, as verificações poderão ainda estar em andamento no volume. Você pode visualizar os resultados das verificações de status de volume para identificar todos os volumes danificados e tomar as ações necessárias.

Quando o Amazon EBS determina que os dados de um volume estão potencialmente inconsistentes, o padrão é desabilitar a E/S do volume de qualquer instância do EC2 anexada, o que ajuda a evitar a corrupção dos dados. Depois que a E/S está desabilitada, a próxima verificação de status falha, e o status do volume é `impaired`. Além disso, você verá um evento que permite que você saiba que a E/S está desabilitada, e que você pode resolver o status danificado do volume habilitando a E/S para o volume. Aguardamos até que você habilite a E/S para oferecer a oportunidade de decidir se você continuará permitindo que suas instâncias usem o volume ou executem uma verificação de consistência usando um comando, como `chkdsk`, antes de fazer isso.

Note

O status do volume é baseado nas verificações de status do volume e não reflete o estado do volume. Portanto, o status do volume não indica volumes no estado `error` (por exemplo, quando um volume está incapacitado de aceitar E/S). Para obter informações sobre estados do volume, consulte [Estado do volume \(p. 1277\)](#).

Se a consistência de um volume específico não for uma preocupação, e você preferir que o volume seja disponibilizado imediatamente se estiver danificado, será possível substituir o comportamento padrão configurando o volume para ativar automaticamente a E/S. Se você ativar o atributo de volume Auto-EnableIO (`autoEnableIO` na API), a verificação do status do volume continua ser aprovada. Além disso, você verá um evento que permite saber que o volume foi determinado como potencialmente inconsistente, mas que sua E/S foi habilitada automaticamente. Isso permite verificar a consistência do volume ou substituí-lo posteriormente.

A verificação do status da performance de E/S compara a performance do volume real com a performance esperada de um volume. Ele alerta você se o volume estiver com uma performance abaixo das expectativas. Essa verificação de status está disponível apenas para volumes SSD de IOPS provisionadas (`io1` e `io2`) anexados a uma instância. A verificação de status não é válida para volumes SSD de uso geral (`gp2` e `gp3`), HDD otimizado para taxa de transferência (`st1`), HDD a frio (`sc1`) ou magnéticos (`standard`). A verificação de status de performance de E/S é realizada uma vez a cada minuto e o CloudWatch coleta esses dados a cada cinco minutos. Pode demorar até cinco minutos a partir do momento em que você anexa um volume de `io1` ou `io2` a uma instância para a verificação de status para relatar o status de performance de E/S.

Important

Durante a inicialização dos volumes de Provisioned IOPS SSD que foram restaurados de snapshots, a performance do volume pode ser reduzida a menos de 50% de seu nível esperado, o que faz com que o volume exiba um estado de `warning` na verificação do status de I/O Performance (Performance de E/S). Isso é esperado, e é possível ignorar o estado de `warning` em volumes de Provisioned IOPS SSD enquanto estiver inicializando esses volumes. Para obter mais informações, consulte [Inicializar volumes de Amazon EBS \(p. 1463\)](#).

A tabela a seguir lista os status dos volumes do Amazon EBS.

Status dos volumes	Status de E/S habilitado	Status de performance de E/S (somente volumes <code>io1</code> e <code>io2</code>)
<code>ok</code>	Habilitado (E/S habilitada ou E/S habilitada automaticamente)	Normal (a performance do volume é a esperada)
<code>warning</code>	Habilitado (E/S habilitada ou E/S habilitada automaticamente)	Degradado (a performance do volume está abaixo das expectativas) Seramente degradado (a performance do volume está muito abaixo das expectativas)
<code>impaired</code>	Habilitado (E/S habilitada ou E/S habilitada automaticamente) Desabilitado (o volume está offline e com recuperação pendente ou está aguardando o usuário habilitar a E/S)	Paralisado (a performance do volume está severamente impactada) Não disponível (incapaz de determinar a performance da E/S porque a E/S é desabilitada)

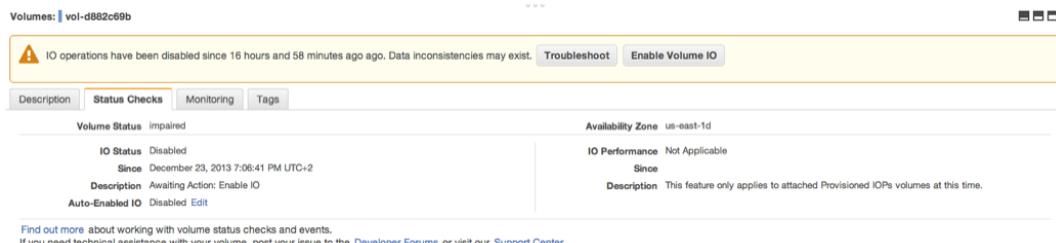
Status dos volumes	Status de E/S habilitado	Status d performance de E/S (somente volumes io1 e io2)
insufficient-data	Habilitado (E/S habilitada ou E/S habilitada automaticamente) Dados insuficientes	Dados insuficientes

Você pode visualizar e trabalhar com verificações de status usando os seguintes métodos.

Console

Para visualizar verificações de status

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes. A coluna Volume Status (Status do volume) lista o status operacional de cada volume.
3. Para visualizar os detalhes de status de um volume, selecione o volume e escolha Status Checks (Verificações de status).



4. Se houver um volume com uma verificação de status com falha (o status é impaired (danificado)), consulte [Trabalhar com um volume danificado \(p. 1286\)](#).

Como alternativa, você pode selecionar Events (Eventos) para visualizar todos os eventos de suas instâncias e volumes. Para obter mais informações, consulte [Eventos de volume do EBS \(p. 1284\)](#).

AWS CLI

Para exibir informações de status do volume

Use um dos seguintes comandos.

- [describe-volume-status](#) (AWS CLI)
- [Get-EC2VolumeStatus](#) (AWS Tools for Windows PowerShell)

Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

Eventos de volume do EBS

Por padrão, quando o Amazon EBS determina que os dados de um volume estão potencialmente inconsistentes, ele desabilita a E/S de qualquer instância do EC2 anexada. Isso faz com que a verificação de status do volume falhe e crie um evento de status de volume que indica a causa da falha.

Para habilitar automaticamente a E/S em um volume com dados potencialmente inconsistentes, altere a configuração do atributo do volume Auto-Enabled IO (Habilitar E/S automaticamente) (`autoEnableIO`)

API). Para obter mais informações sobre como alterar esse atributo, consulte [Trabalhar com um volume danificado \(p. 1286\)](#).

Cada evento inclui uma hora de início, que indica a hora em que o evento ocorreu, e uma duração, que indica por quanto tempo a E/S do volume foi desabilitada. A hora de término é adicionada ao evento quando a E/S do volume é habilitada.

Os eventos de status de volumes incluem uma das seguintes descrições:

Awaiting Action: Enable IO

Os dados do volume estão potencialmente inconsistentes. A E/S é desabilitada para o volume até que você a habilite explicitamente. A descrição do evento é alterada para IO Enabled depois que você habilita a E/S explicitamente.

IO Enabled

As operações de E/S foram habilitadas explicitamente para esse volume.

IO Auto-Enabled

As operações de E/S foram habilitadas automaticamente nesse volume depois da ocorrência de um evento. Recomendamos verificar as inconsistências dos dados antes de continuar a usar os dados.

Normal

Apenas para volumes io1, io2 e gp3. A performance do volume é a esperada.

Degraded

Apenas para volumes io1, io2 e gp3. A performance do volume está abaixo das expectativas.

Severely Degraded

Apenas para volumes io1, io2 e gp3. A performance do volume está muito abaixo das expectativas.

Stalled

Apenas para volumes io1, io2 e gp3. A performance do volume está severamente impactada.

Você pode exibir eventos para seus volumes usando os seguintes métodos.

Console

Para visualizar eventos para seus volumes

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Events. Todas as instâncias e volumes que têm eventos são listados.
3. Você pode filtrar por volume para visualizar somente o status de volumes. Também pode filtrar por tipos específicos de status.
4. Selecione um volume para visualizar seu evento específico.

Event: vol-3682c675

Availability Zone: us-east-1d
Event Type: potential-data-inconsistency
Event Status: Awaiting Action: Enable IO
IO status: IO Disabled
Attached to: i-93aae4ea
Start Time: December 23, 2013 7:09:20 PM UTC+2
End time:

Find out more about [monitoring volume events](#).

AWS CLI

Para visualizar eventos para seus volumes

Use um dos seguintes comandos.

- [describe-volume-status](#) (AWS CLI)
- [Get-EC2VolumeStatus](#) (AWS Tools for Windows PowerShell)

Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

Se você tiver um volume com a E/S desabilitada, consulte [Trabalhar com um volume danificado \(p. 1286\)](#). Se você tiver um volume em que a performance da E/S está abaixo do normal, essa poderá ser uma condição temporária devido a uma ação que você tomou (por exemplo, criar um snapshot de um volume durante o uso de pico, executar o volume em uma instância que não pode oferecer suporte à largura de banda de E/S necessária, acessar dados no volume pela primeira vez etc.).

Trabalhar com um volume danificado

Use as opções a seguir se um volume estiver danificado porque os dados do volume estão potencialmente inconsistentes.

Opções

- [Opção 1: executar uma verificação de consistência no volume anexado a sua instância \(p. 1286\)](#)
- [Opção 2: executar uma verificação de consistência no volume usando outra instância \(p. 1287\)](#)
- [Opção 3. excluir o volume se não precisar mais dele \(p. 1288\)](#)

Opção 1: executar uma verificação de consistência no volume anexado a sua instância

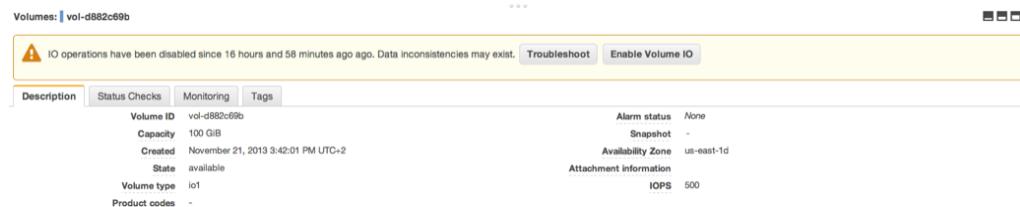
A opção mais simples é habilitar a E/S e executar uma verificação de consistência dos dados no volume enquanto o volume ainda estiver anexado a sua instância do Amazon EC2.

Para executar uma verificação de consistência em um volume anexado

1. Interrompa o uso do volume por todos os aplicativos.
2. Habilite a E/S no volume. Use um dos métodos a seguir.

Console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume no qual habilitar as operações de E/S.
4. No painel de detalhes, escolha Enable Volume IO (Habilitar E/S de volume) e, depois, (Yes, Enable (Sim, habilitar).



AWS CLI

Para habilitar a E/S para um volume com a linha de comando

Você pode usar um dos seguintes comandos para visualizar as informações de eventos de seus volumes do Amazon EBS. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [enable-volume-io](#) (AWS CLI)
- [Enable-EC2VolumeIO](#) (AWS Tools for Windows PowerShell)

3. Verifique os dados no volume.
 - a. Execute o comando chkdsk.
 - b. (Opcional) Analise todos os logs disponíveis da aplicação ou do sistema para verificar se há mensagens de erro relevantes.
 - c. Se o volume estiver insuficiente por mais de 20 minutos, você poderá entrar em contato com o AWS Support Center. Escolha Troubleshoot (Solução de problemas) e, na caixa de diálogo Troubleshoot Status Checks (Verificações de status da solução de problemas), escolha Contact Support (Entrar em contato com o suporte) para enviar um caso de suporte.

Opcão 2: executar uma verificação de consistência no volume usando outra instância

Use o seguinte procedimento para verificar o volume fora de seu ambiente de produção.

Important

Este procedimento pode causar a perda de E/Ss de gravação que foram suspensas quando a E/S do volume foi desabilitada.

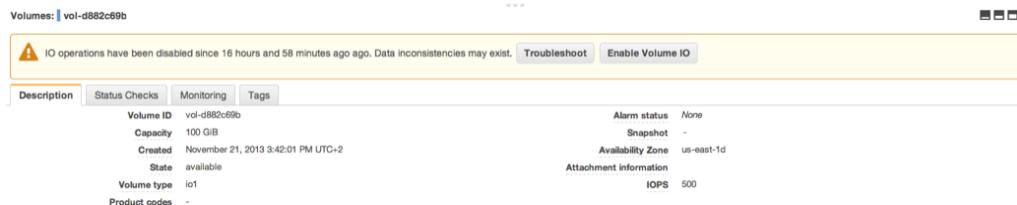
Para executar uma verificação de consistência em um volume isoladamente

1. Interrompa o uso do volume por todas as aplicações.
2. Desanexe o volume da instância. Para obter mais informações, consulte [Desanexar um volume do Amazon EBS de uma instância Windows \(p. 1290\)](#).
3. Habilite a E/S no volume. Use um dos métodos a seguir.

Console

1. No painel de navegação, escolha Volumes.

2. Selecione o volume que você desanexou na etapa anterior.
3. No painel de detalhes, escolha Enable Volume IO (Habilitar E/S de volume) e, depois, (Yes, Enable (Sim, habilitar)).



AWS CLI

Para habilitar a E/S para um volume com a linha de comando

Você pode usar um dos seguintes comandos para visualizar as informações de eventos de seus volumes do Amazon EBS. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [enable-volume-io](#) (AWS CLI)
- [Enable-EC2VolumeIO](#) (AWS Tools for Windows PowerShell)

4. Anexe o volume a outra instância. Para obter mais informações, consulte [Executar sua instância \(p. 417\)](#) e [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#).
5. Verifique os dados no volume.
 - a. Execute o comando chkdsk.
 - b. (Opcional) Analise todos os logs disponíveis da aplicação ou do sistema para verificar se há mensagens de erro relevantes.
 - c. Se o volume estiver insuficiente por mais de 20 minutos, você poderá entrar em contato com o AWS Support Center. Escolha Troubleshoot e, em seguida, na caixa de diálogo de solução de problemas, escolha Contact Support para enviar um caso de suporte.

Opção 3. excluir o volume se não precisar mais dele

Se desejar remover o volume do ambiente, simplesmente exclua-o. Para obter informações sobre como excluir um volume, consulte [Excluir um volume de Amazon EBS \(p. 1293\)](#).

Se você tiver um snapshot recente que faça o backup dos dados no volume, você poderá criar um novo volume do snapshot. Para obter mais informações, consulte [Criar um volume a partir de um snapshot \(p. 1270\)](#).

Trabalhar com o atributo de volume de E/S habilitada automaticamente

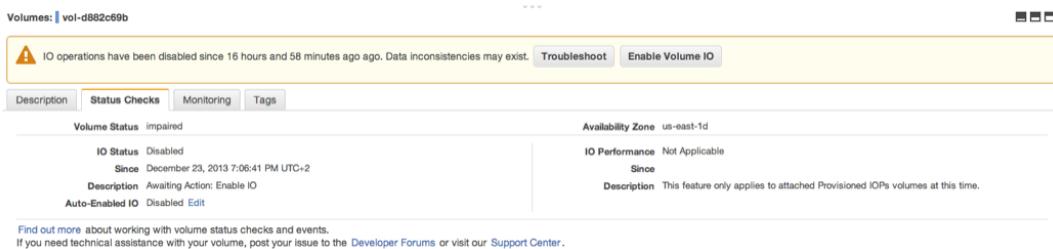
Por padrão, quando o Amazon EBS determina que os dados de um volume estão potencialmente inconsistentes, ele desabilita a E/S de qualquer instância do EC2 anexada. Isso faz com que a verificação de status do volume falhe e crie um evento de status de volume que indica a causa da falha. Se a consistência de um volume específico não for uma preocupação, e você preferir que o volume seja disponibilizado imediatamente se estiver com o status impaired (danificado), será possível substituir o comportamento padrão configurando o volume para ativar automaticamente a E/S. Se você ativar o atributo de volume Auto-Enabled IO (autoEnableIO na API), a E/S entre o volume e a instância será reativada e a verificação de status do volume será aprovada. Além disso, você verá um evento que permite que você saiba que o volume estava em um estado de potencialmente inconsistente, mas que sua E/S foi habilitada automaticamente. Quando esse evento ocorre, você deve verificar a consistência do volume e substitui-lo se necessário. Para obter mais informações, consulte [Eventos de volume do EBS \(p. 1284\)](#).

Você pode exibir e modificar o atributo Auto-Enabled IO (E/S habilitado automaticamente) de um volume usando os seguintes métodos.

Console

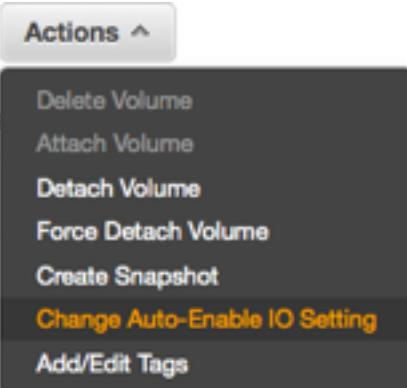
Para visualizar o atributo de E/S habilitado automaticamente de um volume

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume e escolha Status Checks (Verificações de status). O atributo Auto-Enabled IO exibe a configuração atual (Enabled (Habilitada) ou Disabled (Desabilitada)) do seu volume.

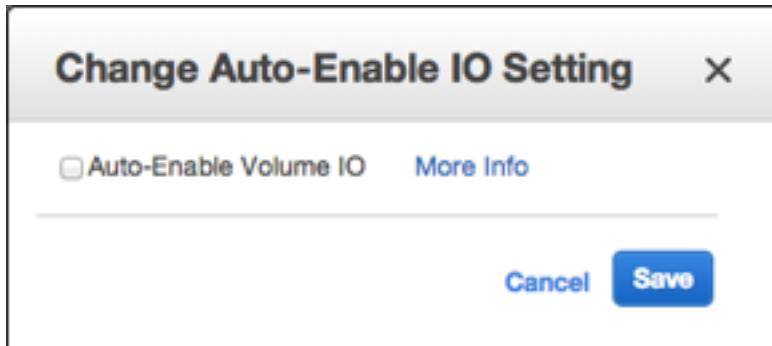


Para modificar o atributo de E/S habilitado automaticamente de um volume

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume e escolha Actions (Ações), Change Auto-Enable IO Setting (Alterar configuração do Auto-Enabled IO). Como alternativa, escolha a guia Status Checks (Verificações de status) e, em Auto-Enabled IO, escolha Edit (Editar).



4. Selecione a caixa de verificações Auto-Enable Volume IO (Habilitar E/S de volume automaticamente) para habilitar automaticamente a E/S de um volume danificado. Para desabilitar o recurso, limpe a caixa de seleção.



5. Escolha Save (Salvar).

AWS CLI

Para visualizar o atributo AutoEnableIO de um volume

Use um dos seguintes comandos.

- [describe-volume-attribute](#) (AWS CLI)
- [Get-EC2VolumeAttribute](#) (AWS Tools for Windows PowerShell)

Para modificar o atributo **autoEnableIO** de um volume

Use um dos seguintes comandos.

- [modify-volume-attribute](#) (AWS CLI)
- [Edit-EC2VolumeAttribute](#) (AWS Tools for Windows PowerShell)

Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#)

Desanexar um volume do Amazon EBS de uma instância Windows

Você precisa desanexar um volume do Amazon Elastic Block Store (Amazon EBS) de uma instância antes de anexá-lo a uma instância diferente ou excluí-lo. Desanexar um volume não afeta os dados no volume.

Para obter informações sobre como separar volumes de uma instância do Linux, consulte [Desanexar um volume de uma instância do Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

- [Considerations \(p. 252\)](#)
- [Desmontar e desanexar um volume \(p. 1291\)](#)
- [Troubleshoot \(p. 1292\)](#)

Considerations

- Você pode separar um volume do Amazon EBS da instância explicitamente ou encerrando a instância. Contudo, se a instância estiver em execução, você deverá primeiro desmontar o volume da instância.

- Se um volume do EBS for o dispositivo raiz de uma instância, você deverá parar a instância antes de separar o volume.
- Você pode anexar novamente um volume que foi desanexado (sem desmontá-lo), mas ele talvez não obtenha o mesmo ponto de montagem. Se havia gravações em andamento no volume quando ele foi desanexado, os dados do volume podem não estar sincronizados
- Após separar um volume, ainda será cobrado o armazenamento de volume, desde que a quantidade de armazenamento exceda o limite de nível gratuito da AWS. Exclua um volume para evitar cobranças adicionais. Para obter mais informações, consulte [Excluir um volume de Amazon EBS \(p. 1293\)](#).

Desmontar e desanexar um volume

Use o procedimento a seguir para desmontar e desanexar um volume de uma instância. Isso pode ser útil quando você precisa anexar o volume a uma instância diferente ou quando você precisar excluir o volume.

Etapas

- [Etapa 1: desmonte o volume. \(p. 1291\)](#)
- [Etapa 2: desanexar o volume da instância. \(p. 1291\)](#)
- [Etapa 3: desinstalar os locais do dispositivo offline \(p. 1292\)](#)

Etapa 1: desmonte o volume.

Na instância do Windows, desmonte o volume, da maneira a seguir.

1. Inicie o utilitário de Gerenciamento de Disco.
 - (Windows Server 2012 e posterior) Na barra de ferramentas, clique com o botão direito do mouse no logo do Windows e escolha Disk Management ((Gerenciamento de disco)).
 - (Windows Server 2008) Escolha Start (Iniciar), Administrative Tools (Ferramentas administrativas), Computer Management (Gerenciamento do computador), Disk Management (Gerenciamento de disco).
2. Clique com o botão direito do mouse no disco (por exemplo, clique com o botão direito do mouse em Disk 1 (Disco 1)) e selecione Offline. Aguarde o status do disco ser alterado para Offline antes de abrir o console do Amazon EC2.

Etapa 2: desanexar o volume da instância.

Para desanexar o volume da instância, use um dos seguintes métodos:

Console

Para separar um volume do EBS usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes.
3. Selecione um volume e escolha Ações, Separar volume.
4. Quando a confirmação for solicitada, escolha Yes, Detach (Sim, separar).

Command line

Para separar um volume do EBS de uma instância usando a linha de comando

Depois de desmontar o volume, você pode usar um dos comandos a seguir para desanexá-lo. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [detach-volume \(AWS CLI\)](#)
- [Dismount-EC2Volume \(AWS Tools for Windows PowerShell\)](#)

Etapa 3: desinstalar os locais do dispositivo offline

Quando você desmonta e desanexa um volume de uma instância, o Windows sinaliza o local do dispositivo como offline. A localização do dispositivo permanece offline após a reinicialização e interromper e reiniciar a instância. Quando você reinicia a instância, o Windows pode montar um dos volumes restantes no local do dispositivo offline. Isso faz com que o volume fique indisponível no Windows. Para evitar que isso aconteça e garantir que todos os volumes estejam conectados a locais de dispositivos online na próxima vez que o Windows for iniciado, execute as seguintes etapas:

1. Na instância, abra o Device Manager (Gerenciador de dispositivos).
2. No Device Manager (Gerenciador de dispositivos), selecione View (Exibir), Show hidden devices (Mostrar dispositivos ocultos).
3. Na lista de dispositivos, expanda o nó Storage controllers (Controladores de armazenamento) .

Os locais dos dispositivos nos quais os volumes desanexados foram montados devem aparecer acinzentados.

4. Clique com o botão direito em cada local do dispositivo acinzentado, selecione Uninstall device (Desinstalar dispositivo) e escolha Uninstall (Desinstalar).

Important

Não marque a caixa de seleção Delete the driver software for this device (Excluir o software do driver para este dispositivo).

Troubleshoot

A seguir estão problemas comuns encontrados ao separar volumes e como resolvê-los.

Note

Para proteger contra a possibilidade de perda de dados, tire um snapshot do seu volume antes de tentar desmontá-lo. A separação forçada de um volume preso pode causar danos ao sistema de arquivos ou aos dados que ele contém ou incapacidade de associar um novo volume usando o mesmo nome de dispositivo, a menos que você reinicialize a instância.

- Se você encontrar problemas ao desanexar um volume com o console do Amazon EC2, pode ser útil usar o comando da CLI describe-volumes para diagnosticar o problema. Para obter mais informações, consulte [describe-volumes](#).
- Se seu volume ficar no estado `detaching`, você poderá forçar a separação escolhendo Força separação. Use essa opção somente como último recurso para separar um volume de uma instância falha ou se você estiver separando um volume com a intenção de excluí-lo. A instância não tem uma oportunidade de nivelar os caches do sistema de arquivos nem os metadados do sistema de arquivos. Se você usar essa opção, deve executar a verificação do sistema de arquivos e os procedimentos de reparo.
- Se você tentou forçar o volume a desanexar várias vezes durante vários minutos e ele permanece no estado `detaching`, é possível publicar uma solicitação de ajuda no [Fórum do Amazon EC2](#). Para ajudar a agilizar uma resolução, inclua o ID do volume e descreva as etapas que já tomou.
- Quando você tenta separar um volume que ainda está montado, o volume pode ficar preso no estado `busy` enquanto está tentando se separar. A seguinte saída de `describe-volumes` mostra um exemplo dessa condição:

```
"Volumes": [
```

```
{  
    "AvailabilityZone": "us-west-2b",  
    "Attachments": [  
        {  
            "AttachTime": "2016-07-21T23:44:52.000Z",  
            "InstanceId": "i-fedc9876",  
            "VolumeId": "vol-1234abcd",  
            "State": "busy",  
            "DeleteOnTermination": false,  
            "Device": "/dev/sdf"  
        }  
        ...  
    ]  
}
```

Quando você encontra esse estado, a separação poderá ser atrasada indefinidamente até que você desmonte o volume, force a separação, reinicialize a instância ou todos os três.

Excluir um volume de Amazon EBS

Depois de não precisar mais de um volume do Amazon EBS, você poderá excluí-lo. Depois da exclusão, seus dados são excluídos e o volume não pode mais ser conectado a nenhuma instância. Contudo, antes de exclusão, você pode armazenar um snapshot de volume, que pode usar para recriar o volume posteriormente.

Note

Não será possível excluir um volume se ele estiver anexado a uma instância. Para excluir um volume, primeiro é necessário desanexá-lo. Para obter mais informações, consulte [Desanexar um volume do Amazon EBS de uma instância Windows \(p. 1290\)](#).

É possível verificar se um volume está anexado a uma instância. No console, na página Volumes, é possível visualizar o estado dos volumes.

- Se um volume estiver anexado a uma instância, ele estará no estado `in-use`.
- Se um volume não estiver anexado a uma instância, ele estará no estado `available`. É possível excluir esse volume.

Você pode excluir um volume do EBS usando um dos métodos a seguir.

Console

Para excluir um volume do EBS usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes.
3. Selecione um volume e escolha Ações, Excluir volume. Se Delete Volume (Excluir volume) estiver esmaecido, o volume estará anexado a uma instância.
4. Na caixa de diálogo de confirmação, escolha Yes, Delete.

AWS CLI

Para excluir um volume do EBS usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [delete-volume](#) (AWS CLI)
- [Remove-EC2Volume](#) (AWS Tools for Windows PowerShell)

Snapshots do Amazon EBS

Você pode fazer backup dos dados nos volumes do Amazon EBS para o Amazon S3 criando snapshots point-in-time. Snapshots são backups incrementais, o que significa que somente os blocos no dispositivo que tiverem mudado depois do snapshot mais recente serão salvos. Isso minimiza o tempo necessário para criar o snapshot e economiza em custos de armazenamento ao não duplicar os dados. Cada snapshot contém todas as informações necessárias para restaurar seus dados (desde o momento em que o snapshot foi tirado) até um volume novo do EBS.

Quando você cria um volume do EBS com base em um snapshot, o novo volume começa como uma réplica exata do volume original usado para criar o snapshot. O volume replicado carrega dados em segundo plano, por isso você pode começar a usá-lo imediatamente. Se você acessar dados que ainda não foram carregados, o volume imediatamente baixa os dados solicitados do Amazon S3 e continua carregando o restante dos dados de volume em segundo plano. Para obter mais informações, consulte [Criar snapshots de Amazon EBS \(p. 1298\)](#).

Ao excluir um snapshot, somente os dados exclusivos desse snapshot serão removidos. Para obter mais informações, consulte [Excluir um snapshot do Amazon EBS \(p. 1314\)](#).

Eventos de snapshot

É possível acompanhar o status de seus snapshots do EBS pelo CloudWatch Events. Para obter mais informações, consulte [Eventos de snapshot do EBS \(p. 1483\)](#).

Snapshots consistentes com aplicação

Usando o Run Command do Systems Manager, você pode gerar snapshots consistentes com a aplicação de todos os volumes do EBS anexados às instâncias do Amazon EC2 no Windows. O processo de snapshot usa o [Serviço de Cópias de Sombra de Volume \(VSS\)](#) do Windows para fazer backups no nível da imagem das aplicações que reconhecem o VSS, incluindo os dados de transações pendentes entre essas aplicações e o disco. Você não precisa desligar as instâncias ou desconectá-las ao fazer backup de todos os volumes anexados. Para obter mais informações, consulte [Criar um snapshot consistente com aplicações VSS](#).

Snapshots de vários volumes

Os snapshots podem ser usados para criar um backup de workloads essenciais, como um banco de dados grande ou um sistema de arquivos que engloba vários volumes do EBS. Com os snapshots de vários volumes, é possível tirar snapshots exatos de momentos específicos, coordenados por dados e consistentes com falhas em vários volumes do EBS associados a uma instância do EC2. Você não precisa mais interromper a instância ou coordenar entre volumes para garantir consistência em caso de falha, pois os snapshots são tirados automaticamente em vários volumes do EBS. Para obter mais informações, consulte as etapas para criar um snapshot de volume do EBS e [Criar snapshots de Amazon EBS \(p. 1298\)](#).

Definição de preço de snapshot

As cobranças dos seus snapshots são baseadas na quantidade de dados armazenados. Como os snapshots são incrementais, a exclusão de um snapshot pode não reduzir os custos de armazenamento de dados. Os dados referenciados exclusivamente por um snapshot são removidos quando esse snapshot é excluído, mas os dados referenciados por outros snapshots são preservados. Para obter mais informações, consulte [Volumes e snapshots do Amazon Elastic Block Store](#) no Manual do usuário do AWS Billing and Cost Management.

Tópicos

- [Como funcionam os snapshots incrementais \(p. 1295\)](#)
- [Copiar e compartilhar snapshots \(p. 1297\)](#)
- [Suporte a criptografia para snapshots \(p. 1298\)](#)
- [Criar snapshots de Amazon EBS \(p. 1298\)](#)
- [Criar um snapshot consistente com aplicação do VSS \(p. 1301\)](#)
- [Excluir um snapshot do Amazon EBS \(p. 1314\)](#)
- [Copiar um snapshot do Amazon EBS. \(p. 1317\)](#)
- [Exibir informações do snapshot do Amazon EBS \(p. 1322\)](#)
- [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#)
- [Amazon EBS local snapshots on Outposts \(p. 1327\)](#)
- [Usar o APIs diretas do EBS para acessar o conteúdo de um snapshot do EBS \(p. 1337\)](#)
- [Automatizar o ciclo de vida do snapshot \(p. 1363\)](#)

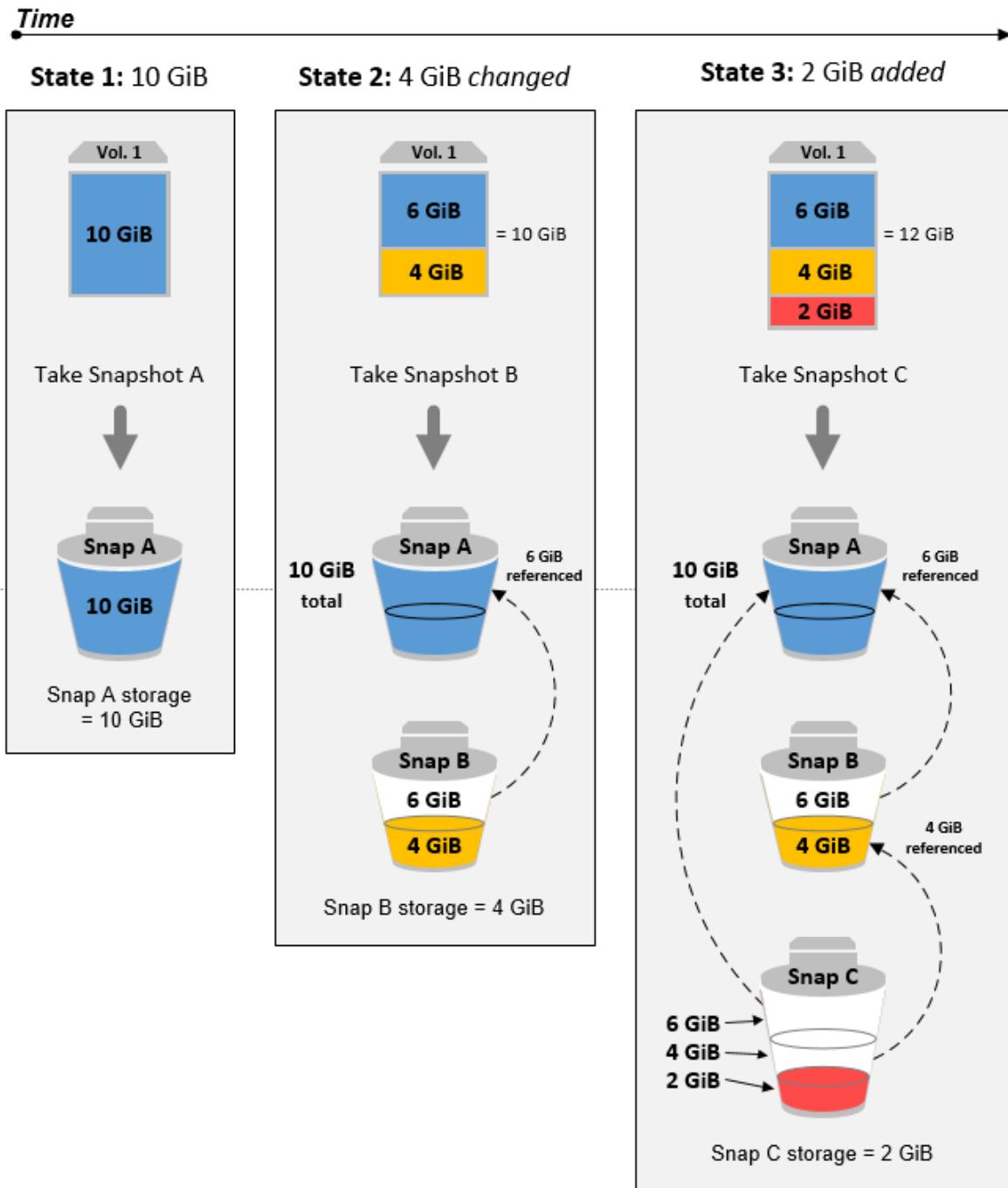
Como funcionam os snapshots incrementais

Esta seção mostra como um snapshot do EBS captura o estado de um volume em um ponto no tempo e como snapshots sucessivos de um volume em constante mudança criam um histórico dessas alterações.

Relações entre múltiplos snapshots do mesmo volume

O diagrama nesta seção mostra o Volume 1 em três pontos no tempo. Um snapshot é retirado de cada um desses três estados de volumes. O diagrama mostra especificamente o seguinte:

- No Estado 1, o volume tem 10 GiB de dados. Como Snap A é o primeiro snapshot criado do volume, todos os 10 GiB de dados devem ser copiados.
- No Estado 2, o volume ainda contém 10 GiB de dados, mas 4 GiB mudaram. O Snap B precisa copiar e armazenar somente os 4 GiB que mudaram após o Snap A ser tirado. Os outros 6 GiB de dados inalterados, que já estão copiados e armazenados no Snap A, são consultados pelo Snap B vez de novamente copiados. Isso é indicado pela seta tracejada.
- No Estado 3, 2 GiB de dados foram adicionados ao volume, totalizando 12 GiB. O Snap C precisa copiar os 2 GiB adicionados após o Snap B ser tirado. Como mostrado pelas setas tracejadas, o Snap C faz referência a 4 GiB de dados armazenados no Snap B e 6 GiB de dados armazenados no Snap A.
- O armazenamento total necessário para os três snapshots é de 16 GiB.



Relações entre snapshots incrementais de diferentes volumes

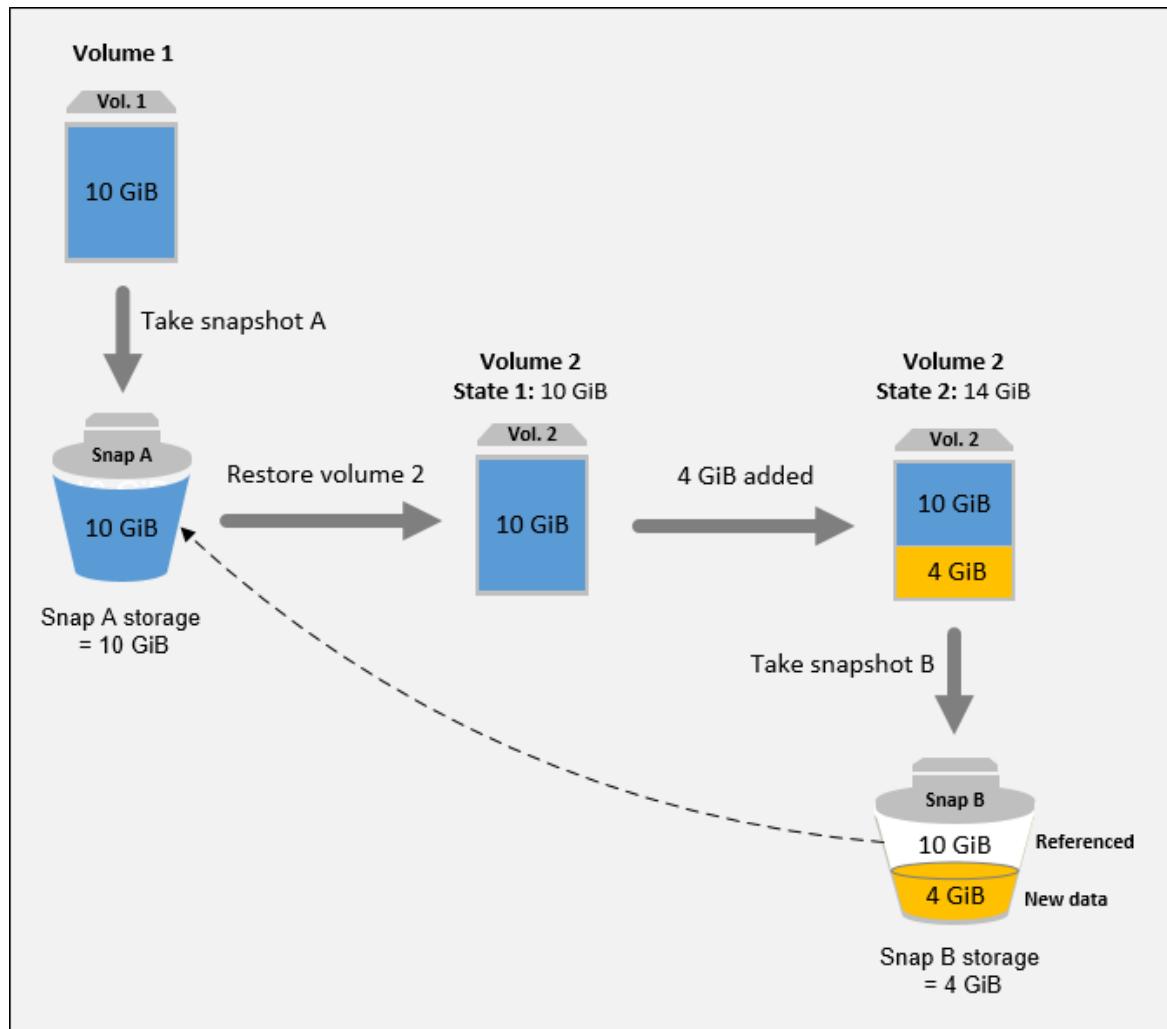
O diagrama nesta seção mostra como snapshots incrementais podem ser obtidos de diferentes volumes.

Important

O diagrama pressupõe que você tem o Vol 1 e criou o Snap A. Se o Vol 1 era de propriedade de outra conta da AWS e essa conta assumiu a propriedade do Snap A e o compartilhou com você, então o Snap B seria um snapshot completo.

1. O Vol 1 tem 10 GiB de dados. Como Snap A é o primeiro snapshot criado do volume, todos os 10 GiB de dados são copiados e armazenados.
2. O Vol 2 é criado do Snap A, por isso é uma réplica exata do Vol 1 no momento em que o snapshot foi criado.
3. Ao longo do tempo, 4 GiB de dados são adicionados ao Vol 2 e seu tamanho total se torna 14 GiB.
4. O Snap B é criado do Vol 2. Para o Snap B, somente os 4 GiB de dados adicionados depois que o volume foi criado do Snap A são copiados e armazenados. Os outros 10 GiB de dados inalterados, que já estão armazenados no Snap A, são consultados pelo Snap B vez de novamente copiados e armazenados.

O Snap B é um snapshot incremental do Snap A, mesmo que tenha sido criado de um volume diferente.



Para obter mais informações sobre como os dados são gerenciados ao excluir um snapshot, consulte [Excluir um snapshot do Amazon EBS \(p. 1314\)](#).

Copiar e compartilhar snapshots

É possível compartilhar um snapshot nas contas da AWS ao modificar suas permissões de acesso. Você pode fazer cópias de seus próprios snapshots e também de snapshots que foram compartilhados com você. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#).

Um snapshot é restrito à região da AWS onde ele foi criado. Após criar um snapshot de um volume do EBS, você pode usá-lo para criar novos volumes na mesma região. Para obter mais informações, consulte [Criar um volume a partir de um snapshot \(p. 1270\)](#). Você também pode copiar os snapshots entre regiões, possibilitando o uso de múltiplas regiões para expansão geográfica, migração de datacenters e recuperação de desastres. Você pode copiar qualquer snapshot acessível que tenha um status de `completed`. Para obter mais informações, consulte [Copiar um snapshot do Amazon EBS \(p. 1317\)](#).

Suporte a criptografia para snapshots

Os snapshots do EBS oferecem suporte completo à criptografia do EBS.

- Snapshots de volumes criptografados são criptografados automaticamente.
- Os volumes criados a partir de snapshots criptografados são criptografados automaticamente.
- Os volumes criados a partir de um snapshot não criptografado pertencente a você ou ao qual você tem acesso podem ser criptografados rapidamente.
- Quando você copia um snapshot não criptografado que você possua, pode criptografá-lo durante o processo de cópia.
- Quando você copia um snapshot criptografado que você possua ou ao qual tenha acesso, pode recriptografá-lo com uma chave diferente durante o processo de cópia.
- O primeiro snapshot que você fizer de um volume criptografado criado a partir de um snapshot não criptografado sempre será um snapshot completo.
- O primeiro snapshot que você fizer de um volume recriptografado, que tem um CMK diferente em relação ao snapshot de origem, sempre será um snapshot completo.

A documentação completa de cenários possíveis de criptografia do snapshot é fornecida em [Criar snapshots de Amazon EBS \(p. 1298\)](#) e em [Copiar um snapshot do Amazon EBS \(p. 1317\)](#).

Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).

Criar snapshots de Amazon EBS

Para criar um snapshot consistente com aplicação, consulte [Criar um snapshot consistente com aplicação do VSS \(p. 1301\)](#).

É possível criar um snapshot de um ponto no tempo de um volume do EBS e usá-lo como uma linha de base para novos volumes ou para backup de dados. Se você fizer snapshots periódicos de um volume, eles serão incrementais — o novo snapshot salvará somente os blocos alterados desde o último snapshot.

Snapshots ocorrem de forma assíncrona; o snapshot de ponto no tempo é criado imediatamente, mas o status do snapshot será `pending` até que ele esteja concluído (quando todos os blocos modificados tiverem sido transferidos para Amazon S3), o que pode levar várias horas para grandes snapshots iniciais ou snapshots subsequentes nos quais muitos blocos tenham sido alterados. Enquanto está sendo concluído, um snapshot em andamento não é afetado pelas leituras e gravações contínuas do volume.

É possível tirar um snapshot de um volume anexado que esteja em uso. No entanto, os snapshots só capturam dados gravados no seu volume do Amazon EBS no momento em que o comando do snapshot é emitido. Isso pode excluir quaisquer dados em cache por quaisquer aplicações ou sistemas operacionais. Se você puder pausar a gravação de qualquer arquivo para o volume por tempo suficiente para tirar um snapshot, seu snapshot deverá estar completo. Contudo, se você não puder pausar todas as gravações do arquivo para o volume, deve desmontar o volume de dentro da instância, emitir o comando de snapshot e remontar o volume para garantir um snapshot consistente e completo. É possível remontar e usar o volume enquanto o status do snapshot for `pending`.

Para facilitar o gerenciamento de snapshots, você pode marcar os snapshots durante a criação ou adicionar tags posteriormente. Por exemplo, você pode aplicar tags que descrevem o volume original a partir do qual o snapshot foi criado ou o nome do dispositivo usado para associar o volume original a uma instância. Para obter mais informações, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

Criptografia de snapshot

Os snapshots tirados dos volumes criptografados são criptografados automaticamente. Os volumes criados a partir de snapshots criptografados também são criptografados automaticamente. Os dados nos seus volumes criptografados e em quaisquer snapshots associados estão protegidos em repouso e em movimento. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1422\)](#).

Por padrão, só você pode criar volumes a partir dos snapshots que possui. Contudo, você pode compartilhar seus snapshots não criptografados com contas específicas da AWS ou compartilhá-los com toda a comunidade AWS tornando eles públicos. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#).

É possível compartilhar um snapshot criptografado somente com as contas da AWS específicas. Para que outros usem o snapshot compartilhado e criptografado, é preciso também compartilhar a chave CMK usada para criptografá-lo. Os usuários com acesso ao seu snapshot criptografado devem criar sua própria cópia pessoal e usar essa cópia. Sua cópia de um snapshot compartilhado e criptografado também pode ser recriptografada usando uma chave diferente. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#).

Snapshots de vários volumes

É possível criar snapshots de vários volumes, que são snapshots point-in-time para todos os volumes do EBS anexados a uma instância do EC2. Também é possível criar políticas de ciclo de vida para automatizar a criação e a retenção de snapshots de vários volumes. Para obter mais informações, consulte [Amazon Data Lifecycle Manager \(p. 1363\)](#).

Depois que os snapshots são criados, cada snapshot é tratado como um snapshot individual. Você pode realizar todas as operações de snapshot, como restaurar, excluir e copiar entre regiões ou contas, assim como o faria com um único snapshot de volume. Também é possível marcar os snapshots de vários volumes como você faria com um único snapshot de volume. Recomendamos marcar os snapshots de vários volumes para gerenciá-los coletivamente durante a restauração, cópia ou retenção.

Os snapshots de vários volumes e consistentes com falhas normalmente são restaurados como um conjunto. Isso é útil para identificar os snapshots que estão em um conjunto consistente com falhas marcando seu conjunto com o ID da instância, o nome ou outros detalhes relevantes. Também é possível optar por copiar automaticamente as tags do volume de origem nos snapshots correspondentes. Isso ajuda a definir os metadados do snapshot, como políticas de acesso, informações de anexo e alocação de custos, de acordo com o volume de origem.

Depois de serem criados, os snapshots serão exibidos no console do EC2 criado no ponto no tempo exato.

Se houver falha em algum snapshot do conjunto de snapshots de múltiplos volumes, todos os outros snapshots exibirão um status de erro e um evento `createSnapshots` do CloudWatch com um resultado `failed` será enviado para sua conta da AWS. Para obter mais informações, consulte [Criar snapshots \(createSnapshots\) \(p. 1483\)](#).

Amazon Data Lifecycle Manager

Você pode criar, reter e excluir snapshots manualmente ou usar o Amazon Data Lifecycle Manager para gerenciar os snapshots para você. Para obter mais informações, consulte [Amazon Data Lifecycle Manager \(p. 1363\)](#).

Considerations

As seguintes considerações se aplicam à criação de snapshots:

- Para criar um snapshot para um volume do EBS que serve como dispositivo raiz, interrompa a instância antes de tirar o snapshot.
- Não é possível criar snapshots de instâncias para as quais a hibernação está habilitada.

- Não é possível criar snapshots de instâncias hibernadas.
- Embora você possa tirar um snapshot de um volume enquanto um snapshot anterior desse volume esteja no status pending, ter vários snapshots pending de um volume pode resultar em performance reduzida do volume até que o snapshot seja concluído.
- Há um limite de um snapshot pending para um único volume de st1 ou desc1, ou cinco snapshots pending para um único volume dos outros tipos de volume. Se você receber um erro `ConcurrentSnapshotLimitExceeded` ao tentar criar vários snapshots simultâneos do mesmo volume, aguarde até que um ou mais snapshots pending sejam concluídos antes de criar outro snapshot desse volume.
- Quando um snapshot é criado de um volume com um código de produto do AWS Marketplace , esse código é propagado para o snapshot.

Criar um snapshot

Para criar um snapshot do volume especificado, use um dos métodos a seguir.

Console

Para criar um snapshot usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Snapshots em Elastic Block Store no painel de navegação.
3. Escolha Create Snapshot (Criar snapshot).
4. Em Select resource type (Selecionar tipo de recurso), escolha Volume.
5. Em Volume, selecione o volume.
6. (Opcional) Insira uma descrição para o snapshot.
7. (Opcional) Escolha Add Tag (Adicionar tag) para adicionar tags ao seu snapshot. Para cada tag, forneça uma chave e um valor.
8. Escolha Create Snapshot (Criar snapshot).

AWS CLI

Para criar um snapshot usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- `create-snapshot` (AWS CLI)
- `New-EC2Snapshot` (AWS Tools for Windows PowerShell)

Criar um snapshot de vários volumes

Para criar um snapshot dos volumes de uma instância, use um dos métodos a seguir.

Console

Para criar snapshots de vários volumes usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Snapshots em Elastic Block Store no painel de navegação.
3. Escolha Create Snapshot (Criar snapshot).
4. Em Select resource type (Selecionar tipo de recurso), escolha Instance (Instância).

5. Selecione o ID da instância para a qual deseja criar backups simultâneos para todos os volumes do EBS anexados. Os snapshots de vários volumes permitem até 40 volumes do EBS por instância.
6. (Opcional) Defina Exclude root volume (Excluir volume raiz).
7. (Opcional) Defina o sinalizador Copy tags from volume (Copiar tags do volume) para copiar automaticamente as tags do volume de origem nos snapshots correspondentes. Isso define os metadados do snapshot, como políticas de acesso, informações de anexo e alocação de custos, para corresponderem com o volume de origem.
8. (Opcional) Escolha Add Tag (Adicionar tag) para adicionar tags ao seu snapshot. Para cada tag, forneça uma chave e um valor.
9. Escolha Create Snapshot (Criar snapshot).

AWS CLI

Para criar snapshots de vários volumes usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [create-snapshots](#) (AWS CLI)
- [New-EC2SnapshotBatch](#) (AWS Tools for Windows PowerShell)

Como criar um snapshot consistente com a aplicação usando o comando de execução do Systems Manager

Use o comando de execução do Systems Manager para tirar snapshots consistentes com a aplicação de todos os volumes do EBS anexados às instâncias do Windows do Amazon EC2. O processo de snapshot usa o [Serviço de Cópias de Sombra de Volume \(VSS\)](#) do Windows para fazer backups no nível da imagem dos aplicativos que reconhecem o VSS, incluindo os dados de transações pendentes entre esses aplicativos e o disco. Você não precisa desligar as instâncias ou desconectá-las ao fazer backup de todos os volumes anexados. Para obter mais informações, consulte [Criar um snapshot consistente com aplicação do VSS \(p. 1301\)](#).

Se todos os snapshots forem concluídos corretamente, um evento `createSnapshots` do CloudWatch com um resultado `succeeded` será enviado para sua conta da AWS. Se houver falha em algum snapshot do conjunto de snapshots de múltiplos volumes, todos os outros snapshots exibirão um status de erro e um evento `createSnapshots` do CloudWatch com um resultado `failed` será enviado para sua conta da AWS. Para obter mais informações, consulte [Criar snapshots \(createSnapshots\) \(p. 1483\)](#).

Como trabalhar com snapshots do EBS

Você pode copiar snapshots, compartilhar snapshots e criar volumes de snapshots. Para obter mais informações, consulte:

- [Copiar um snapshot do Amazon EBS. \(p. 1317\)](#)
- [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#)
- [Criar um volume a partir de um snapshot \(p. 1270\)](#)

Criar um snapshot consistente com aplicação do VSS

Você pode obter snapshots consistentes com a aplicação de todos os volumes do Amazon EBS anexados ao seu Windows nas instâncias do Amazon EC2 usando o [Run Command do AWS Systems Manager](#). O processo do snapshot usa o Windows [Volume Shadow Copy Service \(VSS\)](#) do Windows para fazer

backups no nível de imagem de aplicações habilitadas para VSS. Os snapshots incluem dados das transações pendentes entre essas aplicações e o disco. Além disso, você não precisa desligar as instâncias ou desconectá-las quando precisar fazer backup de todos os volumes anexados.

Não existem custos adicionais para usar snapshots do EBS habilitados para VSS. Você paga apenas pelos snapshots do EBS criados pelo processo de backup. Para obter mais informações, consulte [Como é calculada a fatura de snapshot do EBS?](#)

Tópicos

- [Como funcionam \(p. 1302\)](#)
- [Antes de começar \(p. 1302\)](#)
- [Conceitos básicos \(p. 1303\)](#)
- [Criar um snapshot consistente com aplicação do VSS usando a AWS CLI, o AWS Tools for Windows PowerShell ou o documento AWSEC2-ManageVssIO do SSM \(p. 1308\)](#)
- [Para restaurar volumes por meio de snapshots do EBS habilitados para VSS \(p. 1313\)](#)
- [AWSHistórico de versões do pacote de componentes do VSS \(p. 1314\)](#)

Como funcionam

O processo para fazer snapshots de EBS consistentes com a aplicação e habilitados para VSS é formado pelas etapas a seguir.

1. Concluir os pré-requisitos do Systems Manager.
2. Insira os parâmetros para o documento do SSM `AWSEC2-CreateVssSnapshot` e execute esse documento usando o Run Command. Você não pode criar um snapshot do EBS habilitado para VSS para um volume específico. No entanto, você pode especificar um parâmetro para excluir o volume de inicialização do processo de backup.
3. O agente VSS em sua instância coordena todas as operações de E/S em andamento para a execução de aplicações.
4. O sistema libera todos os buffers de E/S e temporariamente todas as operações de E/S. A pausa dura no máximo dez segundos.
5. Durante essa pausa, o sistema cria snapshots de todos os volumes anexados à instância.
6. A pausa é suspensa e as operações de E/S são retomadas.
7. O sistema adiciona todos os snapshots recém-criados à lista de snapshots do EBS. O sistema marca todos os snapshots do EBS habilitados para VSS que foram criados com êxito por esse processo com `AppConsistent:true`. Essa tag ajuda a identificar os snapshots criados por esse processo, em contraposição a outros processos. Se o sistema encontrar um erro, o snapshot criado por esse processo não incluirá a tag `AppConsistent: true`.
8. Se for necessário restaurar usando um snapshot, você poderá usar o processo padrão do EBS de criação de um volume por meio de um snapshot ou restaurar todos os volumes para uma instância usando um script de exemplo, que é descrito posteriormente nesta seção.

Antes de começar

Antes de criar snapshots do EBS habilitados para VSS usando o Executar comando, examine os requisitos e limitações a seguir e execute as tarefas necessárias.

Important

O pacote AWSVSSComponents e os documentos `AWSEC2-CreateVssSnapshot` e `AWSEC2-ManageVssIO` do SSM não mais recebem atualizações para o Windows Server 2008 R2. O pacote AWSVSSComponents é compatível com o Windows Server 2008 R2 até a versão 1.3.1.0 e nenhuma versão posterior.

Você pode consultar a versão mais recente do Windows 2008 R2 compatível com os documentos AWSEC2–CreateVssSnapshot e AWSEC2–ManageVssIO do SSM usando a API GetDocument e especificando 2008R2 para o –VersionName. Por exemplo:

```
Get-SSMDocument –Name AWSEC2–CreateVssSnapshot –VersionName "2008R2"
```

Amazon EC2 Requisitos de instância do Windows

Os snapshots do EBS habilitados para VSS são comportados para instâncias que executam o Windows Server 2012 ou posterior. Verifique se suas instâncias atendem a todos os requisitos para do Amazon EC2 Windows. Para obter mais informações, consulte [Configurar o AWS Systems Manager](#) no Guia do usuário do AWS Systems Manager

Versão do .NET Framework

O pacote AWSVssComponents requer o .NET Framework versão 4.6 ou posterior. Se estiver utilizando o Windows 2012 ou 2012 R2, a versão padrão do .NET Framework é anterior à 4.6, e será necessário instalar a versão 4.6 ou posterior utilizando o Windows Update.

Versão do SSM Agent

Atualize suas instâncias para usar o SSM Agent versão 2.2.58.0 ou posterior. Se estiver usando uma versão mais antiga do SSM Agent, poderá atualizá-lo usando o Executar comando. Para obter mais informações, consulte [Atualizar o SSM Agent usando o Run Command](#) no Manual do usuário do AWS Systems Manager.

AWS Tools for Windows PowerShell version

Certifique-se de que sua instância esteja executando a versão 3.3.48.0 ou posterior do AWS Tools for Windows PowerShell. Para verificar o número de versão, execute o comando a seguir na instância:

```
Get-AWSPowerShellVersion
```

Se for necessário atualizar a versão do Tools for Windows PowerShell em sua instância, consulte [Instalar o AWS Tools for Windows PowerShell em um computador baseado em Windows](#) no Manual do usuário do AWS Tools for Windows PowerShell.

Conceitos básicos

Tais instruções sobre como instalar os componentes do VSS e executar um snapshot consistentemente com aplicação dos volumes do EBS anexados a uma instância do Windows no EC2. Para obter mais informações, consulte [Conceitos básicos das instâncias do Windows do Amazon EC2](#).

Tópicos

- [Como criar uma função do IAM para snapshots habilitados para VSS \(p. 1303\)](#)
- [Faça download e instale os componentes do VSS na instância do Windows no EC2 \(p. 1305\)](#)
- [Criar um snapshot consistente com aplicação do VSS usando o console \(p. 1306\)](#)

Como criar uma função do IAM para snapshots habilitados para VSS

Os procedimentos a seguir descrevem como trabalhar com políticas do IAM e funções do IAM. Essa política permite que o Systems Manager crie snapshots, marque esses snapshots e anexe metadados como um ID de dispositivo às tags de snapshot padrão criadas pelo sistema.

Para criar uma política do IAM para snapshots habilitados para VSS

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.

2. No painel de navegação, escolha Políticas e, em seguida, Criar política.
3. Na página Create policy (Criar política), selecione a aba JSON e substitua o conteúdo padrão pela política JSON a seguir.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateTags",  
            "Resource": [  
                "arn:aws:ec2:*::snapshot/*",  
                "arn:aws:ec2:*::image/*"  
            ]  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeInstances",  
                "ec2:CreateSnapshot",  
                "ec2:CreateImage",  
                "ec2:DescribeImages"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Se você não pretende definir o parâmetro CreateAmi como True (Verdadeiro), pode omitir `arn:aws:ec2:*::image/*` da primeira instrução da política e omitir `ec2:CreateImage` e `ec2:DescribeImages` da segunda instrução da política.

Se você pretende definir o parâmetro CreateAmi sempre como True, pode omitir `ec2:CreateSnapshot` na segunda declaração de política.

4. Escolha Revisar política.
5. Em Name (Nome), insira um nome para identificar a política, como **VssSnapshotRole** ou outro nome que preferir.
6. (Opcional) Para Description (Descrição), informe a descrição do propósito da função.
7. Escolha Create policy (Criar política).

Use o procedimento a seguir para criar uma função do IAM para snapshots habilitados para VSS. Essa função inclui políticas para o Amazon EC2 e o Systems Manager.

Para criar uma função do IAM para snapshots do EBS habilitados para VSS

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Roles e Create role.
3. Em Select type of trusted entity (Selecionar tipo de entidade confiável), selecione AWS Serviço.
4. Imediatamente em Choose the service that will use this role (Escolher o serviço que usará essa função), selecione EC2 e Next: Permissions (Próximo: permissões).
5. Em Select your use case (Selecionar seu caso de uso), escolha EC2 e Next: Permissions (Próximo: permissões).
6. Na lista de políticas, selecione a caixa ao lado de AmazonSSMManagedInstanceCore. (Digite **SSM** na caixa de texto se você precisar restringir a lista.)
7. Escolha Next: Tags (Próximo: tags).

8. (Opcional) Adicione um ou mais pares de chave-valor de tag para organizar, rastrear ou controlar o acesso para esta função e selecione Next: Review (Próximo: revisar).
9. Em Role name (Nome da função), insira um nome para a nova função, como **VssSnapshotRole** ou outro nome que você preferir.
10. (Opcional) Para Role description (Descrição da função), substitua o texto padrão pela descrição do propósito dessa função.
11. Selecione Create role. O sistema faz com que você retorne para a página Roles.
12. Selecione a função que você acabou de criar. A função Summary page (Página de resumo) é aberta.
13. Escolha Attach policies (Anexar políticas).
14. Pesquise e selecione a caixa ao lado da política que você criou no procedimento anterior, como **VssSnapshotRole** ou outro nome que você escolher.
15. Escolha Anexar política.
16. Anexe essa função às instâncias para as quais você deseja criar snapshots do EBS habilitados para VSS. Para obter mais informações, consulte [Anexar uma função do IAM a uma instância \(p. 1202\)](#).

Faça download e instale os componentes do VSS na instância do Windows no EC2

O Systems Manager requer a instalação de componentes do VSS em suas instâncias. Use o procedimento a seguir para instalar os componentes com o pacote `AWSVssComponents`. O pacote instala dois componentes: um solicitante de VSS e um fornecedor de VSS. Recomendamos que você instale o pacote de componentes do AWS VSS mais recente para melhorar a confiabilidade e a performance de snapshots consistentes com aplicações em suas instâncias do Windows do EC2. Para exibir a versão mais recente do pacote, consulte [AWSHistórico de versões do pacote de componentes do VSS \(p. 1314\)](#).

1. Abra o console do AWS Systems Manager em <https://console.aws.amazon.com/systems-manager/>.
2. No painel de navegação, selecione Executar comando.
3. Selecione Run command (Executar comando).
4. Em Command document (Documento do comando), selecione o botão ao lado de AWS-ConfigureAWSPackage.
5. Em Command parameters (Parâmetros do comando), faça o seguinte:
 - a. Verifique se Action (Ação) está definida como Install (Instalar).
 - b. Em Name (Nome), insira `AwsVssComponents`.
 - c. Em Version (Versão), deixe o campo vazio para que Systems Manager instale a versão mais recente.
6. Em Targets (Destinos), identifique as instâncias nas quais você deseja executar essa operação especificando tags ou selecionando instâncias manualmente.

Note

Se você optar por selecionar manualmente as instâncias e uma instância que você espera visualizar não estiver incluída na lista, consulte [Algumas das minhas instâncias estão ausentes](#) no Manual do usuário do AWS Systems Manager para obter dicas para solução de problemas.

7. Para Other parameters (Outros parâmetros):
 - (Opcional) Em Comment (Comentário), digite informações sobre esse comando.
 - Em Timeout (seconds) (Tempo limite [segundos]), especifique o número de segundos para o sistema aguardar até a falha de execução do comando total.
8. (Opcional) Em Rate control (Controle de taxa):
 - Em Concurrency (Concorrência), especifique um número ou uma porcentagem de instâncias nas quais executar o comando ao mesmo tempo.

Note

Se tiver selecionado destinos escolhendo tags do Amazon EC2 e não tiver certeza de quantas instâncias usam tags selecionadas, limite o número de instâncias que podem executar o documento ao mesmo tempo especificando uma porcentagem.

- Em Error threshold (Limite de erro), especifique quando parar de executar o comando em outras instâncias depois de falhar em alguns ou em uma porcentagem de instâncias. Por exemplo, se você especificar três erros, o Systems Manager deixará de enviar o comando quando o 4º erro for recebido. As instâncias que continuam processando o comando também podem enviar erros.
9. (Opcional) Na seção Output options (Opções de saída), se você quiser salvar a saída de comando em um arquivo, selecione a caixa ao lado de Enable writing to an S3 bucket (Habilitar a gravação em um bucket do S3). Especifique o bucket e os nomes (de pastas) de prefixo (opcional).

Note

As permissões do S3 que concedem a possibilidade de gravar os dados em um bucket do S3 são as do perfil de instância atribuído à instância, e não as do usuário do IAM que realiza essa tarefa. Para obter mais informações, consulte [Criar um perfil de instância do IAM para o Systems Manager](#) no Manual do usuário do AWS Systems Manager.

10. (Opcional) Especifique opções para SNS notifications (Notificações do SNS).

Para obter informações sobre como configurar notificações do Amazon SNS para o Run Command, consulte [Configure Amazon SNS notifications for AWS Systems Manager](#) (Configurar notificações do Amazon SNS para o AWS Systems Manager).

11. Escolha Run.

[Criar um snapshot consistente com aplicação do VSS usando o console](#)

Use o procedimento a seguir para criar um snapshot do EBS habilitado para VSS.

Para criar snapshots do EBS habilitados para VSS usando o console

1. Abra o console do AWS Systems Manager em <https://console.aws.amazon.com/systems-manager/>.
2. No painel de navegação, selecione Executar comando.
3. Selecione Run command (Executar comando).
4. Em Command document (Documento de comando), escolha AWSEC2-CreateVssSnapshot em Document name (Nome do documento) e Latest version at runtime como a Document version (Versão do documento).
5. Em Targets (Destinos), identifique as instâncias nas quais você deseja executar essa operação especificando tags ou selecionando instâncias manualmente.

Note

Se você optar por selecionar manualmente as instâncias e uma instância que você espera visualizar não estiver incluída na lista, consulte [Onde estão minhas instâncias?](#) para obter dicas de solução de problemas.

6. Em Command parameters (Parâmetros do comando), faça o seguinte:
 - a. Escolha uma opção na lista Exclude Boot Volume. Use este parâmetro para excluir volumes de inicialização do processo de backup.
 - b. (Opcional) No campo Description (Descrição), digite uma descrição. Essa descrição é aplicada a qualquer snapshot criado por esse processo.
 - c. (Opcional) Em Tags, digite os valores e as chaves para as tags que você deseja aplicar a qualquer snapshot criado por esse processo. As tags podem ajudar você

a localizar, gerenciar e restaurar volumes em uma lista de snapshots. Por padrão, o sistema preenche o parâmetro tag com uma chave Name. Para o valor dessa chave, especifique um nome que deseja aplicar a snapshots criados por esse processo. Se você desejar especificar outras tags, separe-as usando ponto-e-vírgula. Por exemplo, Key=*Environment*, Value=*Test*;Key=*User*, Value=*TestUser1*.

Recomendamos que você marque esses snapshots. Por padrão, os sistemas marcam os snapshots com o ID do dispositivo e AppConsistent (para indicar snapshots do EBS bem-sucedidos, consistentes com a aplicação e habilitados para VSS).

- d. Em Copy Only (Apenas cópia), selecione True (Verdadeiro) para executar uma operação de backup de apenas cópia. Essa opção é definida como Falsa por padrão, para que o sistema execute uma operação de backup completa. Uma operação de backup completa impede que o sistema quebre a cadeia de backup diferencial no SQL Server ao executar um backup.

Note

Essa opção requer que o provedor AWS VSS versão 1.2.00 ou posterior esteja instalado.

- e. Em No Writers (Sem gravadores), selecione True (Verdadeiro) para excluir gravadores VSS de aplicação do processo de snapshot. Isso pode ajudar você a resolver conflitos com componentes de backup VSS de terceiros. Essa opção é definida como Falsa por padrão.

Note

Essa opção requer que o provedor AWS VSS versão 1.2.00 ou posterior esteja instalado.

- f. Em CreateAMI, escolha True para criar um backup de imagem de máquina da Amazon (AMI) habilitado para VSS, em vez de um snapshot do EBS. Essa opção é definida como Falsa por padrão. Para obter mais informações sobre como criar uma AMI, consulte [Criar uma AMI do Windows a partir de uma instância em execução](#).
- g. (Opcional) Em AmiName, especifique um nome para a AMI criada. Esta opção só será aplicada se a opção CreateAmi estiver definida como True.

7. Para Other parameters (Outros parâmetros):

- Em Comment (Comentário), digite informações sobre esse comando.
- Em Timeout (seconds) (Tempo limite [segundos]), especifique o número de segundos para o sistema aguardar até a falha de execução do comando total.

8. (Opcional) Em Rate control (Controle de taxa):

- Em Concurrency (Concorrência), especifique um número ou uma porcentagem de instâncias nas quais executar o comando ao mesmo tempo.

Note

Se tiver selecionado destinos escolhendo tags do Amazon EC2 e não tiver certeza de quantas instâncias usam tags selecionadas, limite o número de instâncias que podem executar o documento ao mesmo tempo especificando uma porcentagem.

- Em Error threshold (Limite de erro), especifique quando parar de executar o comando em outras instâncias depois de falhar em alguns ou em uma porcentagem de instâncias. Por exemplo, se você especificar três erros, o Systems Manager deixará de enviar o comando quando o 4º erro for recebido. As instâncias que continuam processando o comando também podem enviar erros.

9. (Opcional) Em Output options (Opções de saída) para salvar a saída de comando em um arquivo, selecione a caixa ao lado de Enable writing to an S3 bucket (Habilitar a gravação em um bucket do S3). Especifique o bucket e os nomes (de pastas) de prefixo (opcional).

Note

As permissões do S3 que concedem a possibilidade de gravar os dados em um bucket do S3 são as do perfil de instância atribuído à instância, e não as do usuário do IAM que realiza essa tarefa. Para obter mais informações, consulte [Configurar o Systems Manager](#).

10. (Opcional) Especifique opções para SNS notifications (Notificações do SNS).

Para obter mais informações sobre como configurar notificações do Amazon SNS para o Run Command, consulte [Configurar notificações do Amazon SNS para o AWS Systems Manager](#) no Manual do usuário do AWS Systems Manager.

11. Escolha Run.

Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. Você pode localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então AppConsistent. Se a execução de comando for malsucedida, exiba a saída de comando do Systems Manager para obter detalhes sobre o motivo da falha na execução. Se o comando for concluído com êxito, mas houver falha no backup de um volume específico, você poderá solucionar essa falha na lista de volumes do EBS.

Se o comando falhou e você está usando o Systems Manager com VPC endpoints, verifique se você configurou o endpoint com.amazonaws.**região**.ec2. Sem o endpoint do EC2 definido, a chamada para enumerar os volumes anexados do EBS falha, o que faz com que o comando do Systems Manager falhe. Para obter mais informações sobre como configurar endpoints da VPC com o Systems Manager, consulte [Criar um endpoint da nuvem privada virtual](#) no Manual do usuário do AWS Systems Manager.

Note

Você pode automatizar backups criando uma tarefa de janela de manutenção que use o documento do [AWSEC2–CreateVssSnapshot](#) SSM. Para obter mais informações, consulte [Trabalhar com janela de manutenção \(console\)](#).

Criar um snapshot consistente com aplicação do VSS usando a AWS CLI, o AWS Tools for Windows PowerShell ou o documento AWSEC2–ManageVssIO do SSM

Esta seção inclui procedimentos para criar snapshots do EBS habilitados para VSS usando a AWS CLI ou o AWS Tools for Windows PowerShell. Ela também contém um método avançado para criar snapshots habilitados para VSS usando o documento AWSEC2–ManageVssIO do SSM.

Tópicos

- [Instalar o pacote do VSS usando a AWS CLI ou o Tools for Windows PowerShell \(p. 1308\)](#)
- [Criar snapshots do EBS habilitados para VSS usando a AWS CLI, o Tools for Windows PowerShell ou o documento AWSEC2–ManageVssIO do SSM \(p. 1309\)](#)
- [Soluçaoar problemas de snapshots do EBS habilitados para VSS \(p. 1312\)](#)

[Instalar o pacote do VSS usando a AWS CLI ou o Tools for Windows PowerShell](#)

Use um dos seguintes procedimentos da linha de comando para fazer download e instalar os componentes do VSS na instância do Windows no EC2.

[Instalação do pacote do VSS por meio da AWS CLI](#)

Use o procedimento a seguir para fazer download e instalar o pacote AwsVssComponents em suas instâncias usando o Run Command por meio da AWS CLI. O pacote instala dois componentes: um solicitante de VSS e um fornecedor de VSS. O sistema copia esses componentes para um diretório na instância e, em seguida, registra a DLL do fornecedor como um fornecedor de VSS.

Para instalar o pacote do VSS por meio da AWS CLI

1. Instale e configure a AWS CLI, caso ainda não tenha feito isso.

Para obter mais informações, consulte [To install or upgrade and then configure the AWS CLI](#) (Instalar ou atualizar e depois configurar a AWS CLI) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).

2. Execute o comando a seguir para fazer download e instalar os componentes do VSS necessários para o Systems Manager.

```
aws ssm send-command --document-name "AWS-ConfigureAWSPackage" --instance-ids "i-12345678" --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

Instale o pacote do VSS por meio do Tools for Windows PowerShell

Use o procedimento a seguir para fazer download e instalar o pacote AwsVssComponents em suas instâncias usando o Run Command por meio do Tools for Windows PowerShell. O pacote instala dois componentes: um solicitante de VSS e um fornecedor de VSS. O sistema copia esses componentes para um diretório na instância e, em seguida, registra a DLL do fornecedor como um fornecedor de VSS.

Para instalar o pacote do VSS por meio do AWS Tools for Windows PowerShell

1. Abra o AWS Tools for Windows PowerShell e execute o seguinte comando para especificar suas credenciais. Você deve ter privilégios de administrador no Amazon EC2 ou deve ter recebido a permissão apropriada no IAM. Para obter mais informações, consulte [Configurar o AWS Systems Manager](#) no Manual do usuário do AWS Systems Manager.

```
Set-AWSCredentials -AccessKey key_name -SecretKey key_name
```

2. Execute o seguinte comando para configurar a Região da sua sessão do PowerShell. O exemplo usa a região us-east-2.

```
Set-DefaultAWSRegion -Region us-east-2
```

3. Execute o comando a seguir para fazer download e instalar os componentes do VSS necessários para o Systems Manager.

```
Send-SSMCommand -DocumentName AWS-ConfigureAWSPackage -InstanceId "$instance"-Parameter @{'action'='Install';'name'='AwsVssComponents'}
```

Criar snapshots do EBS habilitados para VSS usando a AWS CLI, o Tools for Windows PowerShell ou o documento [AWSEC2-ManageVssIO](#) do SSM

Use um dos seguintes procedimentos da linha de comando para criar snapshots do EBS habilitados para VSS.

Como criar snapshots do EBS habilitados para VSS usando a AWS CLI

Use o procedimento a seguir para criar snapshots do EBS habilitados para VSS usando a AWS CLI. Ao executar o comando, você pode especificar os parâmetros a seguir:

- Instância (obrigatório): especifique uma ou mais instâncias Windows do Amazon EC2. Você pode especificar manualmente instâncias ou você especificar tags.
- Descrição (opcional): especifique detalhes sobre esse backup.
- Tags (opcional): especifique pares de chave/valor de tags que você deseja atribuir aos snapshots. As tags podem ajudar você a localizar, gerenciar e restaurar volumes em uma lista de snapshots. Por padrão, o sistema preenche o parâmetro tag com uma chave Name. Para o valor dessa chave, especifique um nome que deseja aplicar a snapshots criados por

esse processo. Você também pode adicionar tags personalizadas usando o formato a seguir:
`Key=Environment,Value=Test;Key=User,Value=TestUser1.`

Esse parâmetro é opcional, mas recomendamos que você marque os snapshots. Por padrão, os sistemas marcam os snapshots com o ID do dispositivo e AppConsistent (para indicar snapshots do EBS bem-sucedidos, consistentes com o aplicativo e habilitados para VSS).

- Excluir volume de inicialização (opcional): use esse parâmetro para excluir volumes de inicialização do processo de backup.

Para criar snapshots do EBS habilitados para VSS usando a AWS CLI

1. Instale e configure a AWS CLI, caso ainda não tenha feito isso.

Para obter mais informações, consulte [Instalar ou atualizar e depois configurar a AWS CLI](#) no Manual do usuário do AWS Systems Manager.

2. Execute o comando a seguir para criar snapshots do EBS habilitados para VSS.

```
aws ssm send-command --document-name "AWSEC2-CreateVssSnapshot" --instance-ids "i-12345678" --parameters '{"ExcludeBootVolume": ["False"], "description": ["Description"], "tags": [{"Key=key_name, Value=tag_value}]}
```

Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. Você pode localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então AppConsistent. Se a execução de comando for malsucedida, exiba a saída de comando do para obter detalhes sobre o motivo da falha na execução.

Você pode automatizar backups criando uma tarefa de janela de manutenção que use o documento do AWSEC2-CreateVssSnapshot SSM. Para obter mais informações, consulte [Trabalhar com janelas de manutenção \(console\)](#) no Manual do usuário do AWS Systems Manager.

Criar snapshots do EBS habilitados para VSS usando o AWS Tools for Windows Powershell

Use o procedimento a seguir para criar snapshots do EBS habilitados para VSS usando o AWS Tools for Windows PowerShell. Ao executar o comando, você pode especificar os parâmetros a seguir:

- Instância (obrigatório): especifique uma ou mais instâncias Windows do Amazon EC2. Você pode especificar manualmente instâncias ou você especificar tags.
- Descrição (opcional): especifique detalhes sobre esse backup.
- Tags (opcional): especifique pares de chave/valor de tags que você deseja atribuir aos snapshots. As tags podem ajudar você a localizar, gerenciar e restaurar volumes em uma lista de snapshots. Por padrão, o sistema preenche o parâmetro tag com uma chave Name. Para o valor dessa chave, especifique um nome que deseja aplicar a snapshots criados por esse processo. Você também pode adicionar tags personalizadas usando o formato a seguir:
`Key=Environment,Value=Test;Key=User,Value=TestUser1.`

Esse parâmetro é opcional, mas recomendamos que você marque os snapshots. Por padrão, os sistemas marcam os snapshots com o ID do dispositivo e AppConsistent (para indicar snapshots do EBS bem-sucedidos, consistentes com o aplicativo e habilitados para VSS).

- Excluir volume de inicialização (opcional): use esse parâmetro para excluir volumes de inicialização do processo de backup.

Para criar snapshots do EBS habilitados para VSS usando o AWS Tools for Windows PowerShell

1. Abra o AWS Tools for Windows PowerShell e execute o seguinte comando para especificar suas credenciais. Você deve ter privilégios de administrador no Amazon EC2 ou deve ter recebido a

permissão apropriada no IAM. Para obter mais informações, consulte [Setting Up AWS Systems Manager](#) (Configurar o AWS Systems Manager) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).

```
Set-AWSCredentials -AccessKey key_name -SecretKey key_name
```

2. Execute o comando a seguir para definir a região para sua sessão de PowerShell. O exemplo usa a região us-east-2.

```
Set-DefaultAWSRegion -Region us-east-2
```

3. Execute o comando a seguir para criar snapshots do EBS habilitados para VSS.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId "$instance" -  
Parameter @{'ExcludeBootVolume'='False';'description'='a_description'  
;'tags'='Key=key_name,Value=tag_value'}
```

Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. Você pode localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então AppConsistent. Se a execução de comando for malsucedida, exiba a saída de comando do para obter detalhes sobre o motivo da falha na execução. Se o comando for concluído com êxito, mas houver falha no backup de um volume específico, você poderá solucionar essa falha na lista de snapshots do EBS.

Você pode automatizar backups criando uma tarefa de janela de manutenção que use o documento do AWSEC2-CreateVssSnapshot SSM. Para obter mais informações, consulte [Working with maintenance windows \(console\)](#) (Trabalhar com janelas de manutenção (console)) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).

[Criar snapshots do EBS habilitados para VSS usando o documento AWSEC2-ManageVssIO do SSM \(avançado\)](#)

Você pode usar o script a seguir e o documento predefinido AWSEC2-ManageVssIO do SSM para pausar temporariamente as operações de E/S, criar snapshots do EBS habilitados para VSS e reiniciar as operações de E/S. Esse processo é executado no contexto do usuário que executa o comando. Se o usuário tiver permissão suficiente para criar e marcar snapshots, o AWS Systems Manager poderá criar e marcar snapshots do EBS habilitados para VSS sem precisar de outra função de snapshot do IAM na instância.

Entretanto, o documento AWSEC2-CreateVssSnapshot exige que você atribua a função de snapshot do IAM a cada instância para a qual deseja criar snapshots do EBS. Se não desejar fornecer mais permissões do IAM às suas instâncias por motivo de política ou conformidade, poderá usar o script a seguir.

Antes de começar

Observe os detalhes essenciais a seguir sobre esse processo:

- Esse processo usa um script do PowerShell (`CreateVssSnapshotAdvancedScript.ps1`) para fazer snapshots de todos os volumes das instâncias que você especificar, com exceção dos volumes raiz. Se você precisar fazer snapshots dos volumes raiz, use o documento SSM do AWSEC2-CreateVssSnapshot.
- O script chama o documento AWSEC2-ManageVssIO duas vezes. A primeira vez com o parâmetro `Action` definido como `Freeze`, que pausa todas as operações de E/S nas instâncias. Na segunda vez, o parâmetro `Action` é definido como `Thaw`, que força a retomada das operações de E/S.
- Não tente usar o documento AWSEC2-ManageVssIO sem usar o script `CreateVssSnapshotAdvancedScript.ps1`. A limitação no VSS requer que as ações `Freeze` e `Thaw` sejam chamadas a não mais de dez segundos de distância, e chamar manualmente essas ações sem o script pode gerar erros.

Para criar snapshots do EBS habilitados para VSS usando o documento [AWSEC2-ManageVssIO](#) do SSM

1. Abra o AWS Tools for Windows PowerShell e execute o seguinte comando para especificar suas credenciais. Você deve ter privilégios de administrador no Amazon EC2 ou deve ter recebido a permissão apropriada no IAM. Para obter mais informações, consulte [Setting Up AWS Systems Manager](#) (Configurar o AWS Systems Manager) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).

```
Set-AWSCredentials -AccessKey key_name -SecretKey key_name
```

2. Execute o comando a seguir para definir a região para sua sessão de PowerShell. O exemplo usa a região us-east-2.

```
Set-DefaultAWSRegion -Region us-east-2
```

3. Faça download do arquivo [CreateVssSnapshotAdvancedScript.zip](#) e extraia os conteúdos do arquivo.
4. Abra `CreateVssSnapshotAdvancedScript.ps1` em um editor de texto, edite a chamada de amostra, na parte inferior do script, com um ID válido da instância do EC2, a descrição do snapshot e os valores de tag desejados e execute o script a partir do PowerShell.

Se bem-sucedido, o comando preenche a lista de snapshots do EBS com os novos snapshots. Você pode localizar esses snapshots na lista de snapshots do EBS procurando as tags que especificou ou então `AppConsistent`. Se a execução de comando for malsucedida, exiba a saída de comando do para obter detalhes sobre o motivo da falha na execução. Se o comando tiver sido concluído com êxito, mas tiver havido falha no backup de um volume específico, você poderá solucionar essa falha na lista de volumes do EBS.

Solucionar problemas de snapshots do EBS habilitados para VSS

Geral: verificando os arquivos de log

Se você tiver problemas ou receber mensagens de erro ao criar snapshots do EBS habilitados para VSS, poderá visualizar a saída do comando no console do Systems Manager (Gerenciador de sistemas). Você também pode visualizar os seguintes logs:

- `%ProgramData%\Amazon\SSM\InstanceData\InstanceID\document\orchestration\SSMCommandID\awsrunPowerShellScript\runPowerShellScript\stdout`
- `%ProgramData%\Amazon\SSM\InstanceData\InstanceID\document\orchestration\SSMCommandID\awsrunPowerShellScript\runPowerShellScript\stderr`

Você também pode abrir a aplicação do Windows Event Viewer (Visualizador de Eventos) e escolher Windows Logs (Logs do Windows), Application (Aplicação) para exibir registros adicionais. Para ver eventos especificamente do provedor VSS do EC2 do Windows e do Volume Shadow Copy Service (Serviço de Cópia de Sombra de Volume), filtре por Source (Origem) nos termos `Ec2VssSoftwareProvider VSSE`.

Erro: A conexão do tubo de descongelamento expirou, erro no descongelamento, tempo limite aguardando o VSS Freeze, ou outros erros de tempo limite

O provedor de VSS do Windows EC2 pode acabar devido a atividades ou serviços na instância, impedindo que snapshots habilitados para VSS prossigam em tempo hábil. O Windows VSS Framework fornece uma janela de 10 segundos não configurável durante a qual a comunicação com o sistema de arquivos é pausada. Durante esse tempo, o `AWSEC2-CreateVssSnapshot` captura seus volumes.

Os seguintes itens podem fazer com que o provedor VSS do Windows EC2 seja executado em limites de tempo durante um snapshot:

- E/S excessiva para um volume
- Capacidade de resposta lenta da API do EC2 na instância
- Volumes fragmentados
- Incompatibilidade com algum software antivírus
- Problemas com um gravador de aplicação de VSS
- Quando o Registro de Módulos estiver habilitado para um grande número de módulos do PowerShell, os scripts do PowerShell poderão ser executados com lentidão

Normalmente, ao executar limites de tempo com o comando `AWSEC2-CreateVssSnapshot`, a causa está relacionada à workload na instância sendo muito alta no momento do backup. As ações a seguir podem ajudá-lo a obter um snapshot bem-sucedido:

- Tente novamente o comando `AWSEC2-CreateVssSnapshot` para ver se a tentativa do snapshot é bem-sucedida. Se a nova tentativa for bem-sucedida em alguns casos, reduzir a carga da instância poderá tornar os snapshots mais bem-sucedidos.
- Aguarde um pouco até que a workload na instância diminua e tente novamente o comando `AWSEC2-CreateVssSnapshot`. Como alternativa, você pode tentar capturar snapshots quando a instância é conhecida por estar sob baixa tensão.
- Tente snapshots do VSS quando o software antivírus no sistema estiver desativado. Se isso resolver o problema, consulte as instruções do software antivírus e configure-o para permitir snapshots do VSS.
- Se houver muitas chamadas de API do EC2 sendo feitas no momento do snapshot, a limitação da API pode fazer com que os snapshots demorem muito para serem iniciados. Tente tirar snapshots novamente quando houver menos atividade de API na conta.
- Execute o comando `vssadmin list writers` em um shell e veja se ele relata quaisquer erros no campo `Last error` (Último erro) para qualquer gravador no sistema. Se algum gravador relatar um erro de tempo esgotado, tente novamente capturar snapshots quando a instância estiver com menos carga.
- Se um ou mais módulos do PowerShell tiverem políticas de grupo que habilitam o log do módulo do PowerShell, tente desabilitar temporariamente o log antes de tirar um snapshot.

Para restaurar volumes por meio de snapshots do EBS habilitados para VSS

Você pode usar o script `RestoreVssSnapshotSampleScript.ps1` para restaurar volumes em uma instância por meio de snapshots do EBS habilitados para VSS. Esse script executa as seguintes tarefas:

- Interrompe uma instância
- Remove todos os discos existentes da instância (exceto o volume de inicialização, se ele tiver sido excluído)
- Cria novos volumes por meio dos snapshots
- Anexa os volumes à instância usando a tag do ID do dispositivo no snapshot
- Reinicia a instância

Important

O script a seguir separa todos os volumes anexados a uma instância e, em seguida, cria novos volumes por meio de um snapshot. É essencial fazer um backup correto da instância. Os volumes antigos não são excluídos. Se desejar, você pode editar o script para excluir os volumes antigos.

Para restaurar volumes por meio de snapshots do EBS habilitados para VSS

1. Abra o AWS Tools for Windows PowerShell e execute o seguinte comando para especificar suas credenciais. Você deve ter privilégios de administrador no Amazon EC2 ou deve ter recebido a

permissão apropriada no IAM. Para obter mais informações, consulte [Configurar o AWS Systems Manager](#) no Manual do usuário do AWS Systems Manager.

```
Set-AWSCredentials -AccessKey key_name -SecretKey key_name
```

2. Execute o seguinte comando para configurar a Região da sua sessão do PowerShell. O exemplo usa a região us-east-2.

```
Set-DefaultAWSRegion -Region us-east-2
```

3. Faça download do arquivo [RestoreVssSnapshotSampleScript.zip](#) e extraia o conteúdo dele.
4. Abra [RestoreVssSnapshotSampleScript.zip](#) em um editor de texto e edite a chamada de amostra na parte inferior do script com um ID válido de instância do EC2 e o ID do snapshot do EBS. Depois, execute o script pelo PowerShell.

AWSHistórico de versões do pacote de componentes do VSS

A tabela a seguir descreve as versões lançadas do pacote de componentes do AWS VSS.

Versão	Detalhes	Data de lançamento
1.3.1.0	<ul style="list-style-type: none">Correção de snapshots com falha em controladores de domínio em relação a um erro de registro de gravador NTDS VSS.Correção do erro do agente VSS ao desinstalar o provedor VSS versão 1.0.	6 de fevereiro de 2020
1.3.00	<ul style="list-style-type: none">Registro aprimorado reduzindo a verbosidade indesejada.Correção de problemas de regionalização durante a instalação.Correção de códigos de retorno para algumas condições de erro de registro do provedor.Correção de vários problemas de instalação.	19 de março de 2019
1.2.00	<ul style="list-style-type: none">Adição de parâmetros de linha de comando -nw (sem gravadores) e -copy (somente cópia) ao agente.Correção de erros de log de eventos causados por chamadas inadequadas de alocação de memória.	15 de novembro de 2018
1.1	Correção de <code>AwsVssProvider.dll</code> sendo usado incorretamente como o provedor padrão de Backup e Restauração do Windows.	12 de dezembro de 2017
1,0	Versão inicial.	20 de novembro de 2017

Excluir um snapshot do Amazon EBS

Depois de não precisar mais de um snapshot do Amazon EBS de um volume, você poderá excluí-lo. A exclusão de um snapshot não tem efeito sobre o volume. A exclusão de um volume não efeita sobre os snapshots feitos deles.

Exclusão incremental de snapshot

Se você gera snapshots periódicos de um volume, eles são incrementais. Isso significa que somente os blocos do dispositivo que foram modificados depois do último snapshot são salvos no novo snapshot. Mesmo que os snapshots sejam salvos de forma incremental, o processo de exclusão de snapshots foi projetado de forma que você precise reter somente o snapshot mais recente a fim de criar volumes.

Se os dados estivessem presentes em um volume mantido em um snapshot anterior ou em uma série de instantâneos e esses dados forem posteriormente excluídos do volume posteriormente, os dados ainda serão considerados dados exclusivos dos snapshots anteriores. Os dados exclusivos serão excluídos da sequência de snapshots apenas se todos os snapshots que fazem referência aos dados exclusivos forem excluídos.

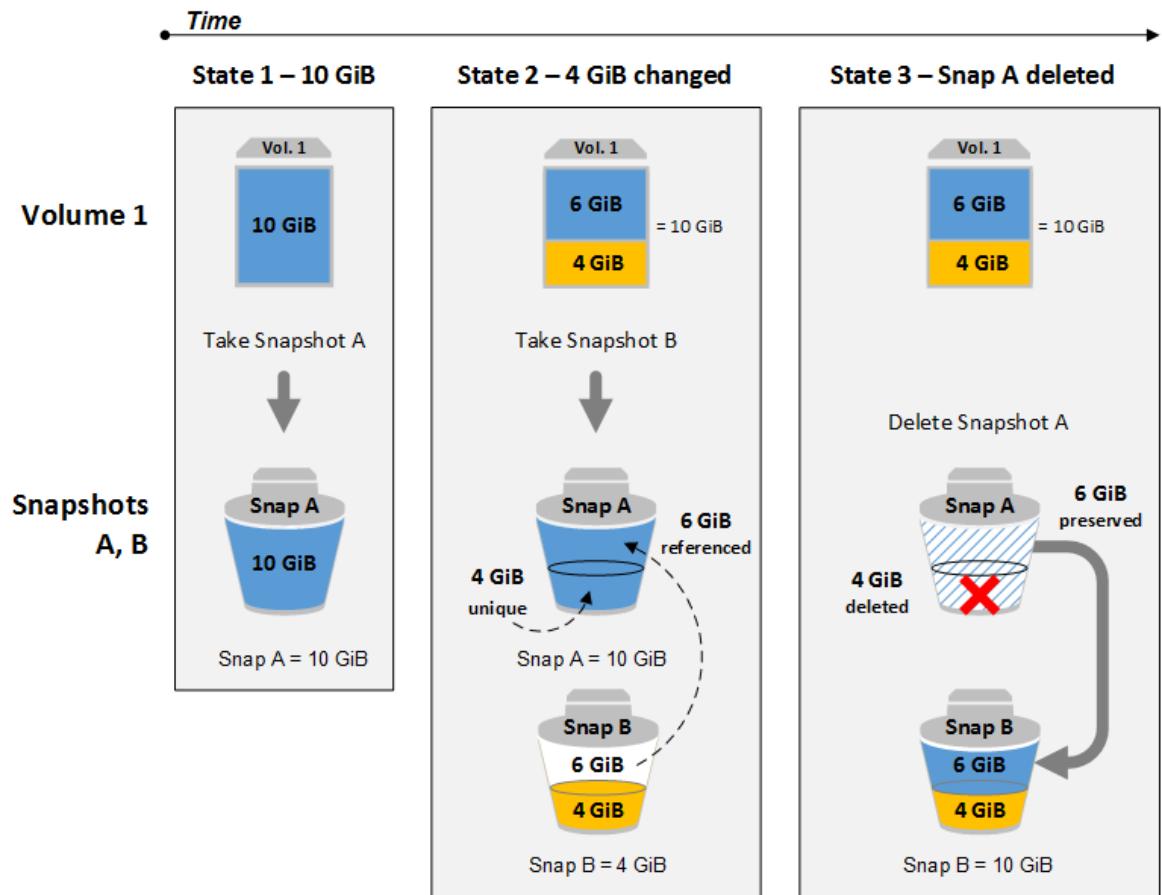
Ao excluir um snapshot, somente os dados mencionados exclusivamente por esse snapshot são removidos. Os dados exclusivos só serão excluídos se todos os snapshots que fazem referência a eles forem excluídos. A exclusão de snapshots anteriores de um volume não afeta sua capacidade de criar volumes de snapshots posteriores desse volume.

A exclusão de um snapshot pode não reduzir os custos de armazenamento de dados de sua organização. Outros snapshots podem fazer referência aos dados desse snapshot e os dados referenciados serão sempre preservados. Se você excluir um snapshot contendo dados usados por um snapshot mais recente, os custos associados aos dados referenciados são alocados ao snapshot posterior. Para obter mais informações sobre como os snapshots armazenam dados, consulte [Como funcionam os snapshots incrementais \(p. 1295\)](#) e o exemplo a seguir.

No diagrama a seguir, Volume 1 é mostrado em três pontos no tempo. Um snapshot capturou os dois primeiros estados e, no terceiro, um snapshot foi excluído.

- No estado 1, o volume tem 10 GiB de dados. Como Snap A é o primeiro snapshot criado do volume, todos os 10 GiB de dados devem ser copiados.
- No Estado 2, o volume ainda contém 10 GiB de dados, mas 4 GiB mudaram. O Snap B precisa copiar e armazenar somente os 4 GiB que mudaram após o Snap A ser tirado. Os outros 6 GiB de dados inalterados, que já estão copiados e armazenados no Snap A, são consultados pelo Snap B vez de (novamente) copiados. Isso é indicado pela seta tracejada.
- No estado 3, o volume não foi alterado desde o Estado 2, mas o Snapshot A foi excluído. Os 6 GiB de dados armazenados no Snapshot A que foram mencionados pelo Snapshot B foram movidos para o Snapshot B, como mostrado pela seta preenchida. Como resultado, será cobrado de você ainda o armazenamento de 10 GiB de dados – 6 GiB de dados inalterados preservados do Snap A e 4 GiB de dados alterados do Snap B.

Exclusão de um snapshot com alguns de seus dados mencionados por outro snapshot



Considerations

As seguintes considerações se aplicam à exclusão de snapshots:

- Você não pode excluir um snapshot do dispositivo raiz de um volume do EBS usado por um AMI registrado. Você deve primeiro cancelar a AMI antes de excluir o snapshot. Para obter mais informações, consulte [Cancelar o registro da AMI do Windows \(p. 55\)](#).
- Não é possível excluir um snapshot gerenciado pelo serviço do AWS Backup usando o Amazon EC2. Em vez disso, use o AWS Backup para excluir os pontos de recuperação correspondentes no cofre de backup.
- Você pode criar, reter e excluir snapshots manualmente ou usar o Amazon Data Lifecycle Manager para gerenciar os snapshots para você. Para obter mais informações, consulte [Amazon Data Lifecycle Manager \(p. 1363\)](#).
- Embora você possa excluir um snapshot que ainda está em andamento, o snapshot deve ser concluído antes de a exclusão entrar em vigor. Isso pode levar muito tempo. Se você também estiver no limite de snapshots simultâneos e tentar criar um snapshot adicional, poderá obter o erro `ConcurrentSnapshotLimitExceeded`. Para obter mais informações, consulte [Service Quotas](#) para o Amazon EBS na Referência geral do Amazon Web Services.

Excluir um snapshot

Para excluir um snapshot, use um dos métodos a seguir.

Console

Para excluir um snapshot usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione Snapshots no painel de navegação.
3. Selecione um snapshot e escolha Excluir na lista Ações.
4. Selecione Sim, excluir.

AWS CLI

Para excluir um snapshot usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [delete-snapshot](#) (AWS CLI)
- [Remove-EC2Snapshot](#) (AWS Tools for Windows PowerShell)

Excluir um snapshot de vários volumes

Para excluir snapshots de vários volumes, recupere todos os snapshots do conjunto de snapshots de vários volumes usando a etiqueta aplicada ao conjunto quando os snapshots foram criados. Depois, exclua os snapshots individualmente.

A exclusão de snapshots individuais no conjunto de snapshots de vários volumes não será impedida. Se você excluir um snapshot enquanto ele estiver no `pending` state, somente esse snapshot será excluído. Os outros snapshots do conjunto de instantâneos de vários volumes ainda serão concluídos corretamente.

Copiar um snapshot do Amazon EBS.

Com o Amazon EBS, você pode criar snapshots de pontos no tempo dos volumes, que nós armazenamos para você em Amazon S3. Depois que um snapshot é criado e copiado para o Amazon S3 (quando o status do snapshot é `completed`), você pode copiá-lo de uma região da AWS para outra ou dentro da mesma região. A criptografia do lado do servidor do Amazon S3 (AES de 256 bits) protege os dados de um snapshot em trânsito durante uma operação de cópia. A cópia do snapshot recebe um ID diferente do ID do snapshot original.

Para copiar snapshots de vários volumes para outra região da AWS, recupere os snapshots usando a etiqueta aplicada ao conjunto de snapshots de vários volumes quando você o criou. Depois, copie cada snapshot para outra região.

Caso queira que outra conta consiga copiar seu snapshot, você deve ao modificar as permissões do snapshot para permitir acesso a essa conta ou tornar o snapshot público para que todas as contas da AWS possam copiá-lo. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#).

Para obter informações sobre como copiar um snapshot do Amazon RDS, consulte [Cópia de um DB Snapshot](#) no Guia do usuário da Amazon RDS.

Casos de uso

- Expansão geográfica: execute suas aplicações em uma nova região da AWS.
- Migração: move uma aplicação para uma nova região, de forma a permitir melhor disponibilidade e minimizar os custos.

- Recuperação de desastres: faça backup dos seus dados e logs em locais geográficos diferentes e intervalos regulares. Em caso de desastre, você pode restaurar suas aplicações usando backups de ponto no tempo armazenados na região secundária. Isso minimiza a perda de dados e o tempo de recuperação.
- Criptografia: criptografe um snapshot não criptografado previamente, altere a chave com a qual o snapshot foi criptografado ou crie uma cópia de sua propriedade para criar um volume a partir dela (para snapshots criptografados que foram compartilhados com você).
- Retenção de dados e requisitos de auditoria: copie seus snapshots do EBS criptografados de uma conta da AWS para outra para preservar os logs de dados ou outros arquivos para auditoria ou retenção de dados. Usar uma conta diferente ajuda a evitar exclusões acidentais de snapshots e protege você se sua conta principal da AWS estiver comprometida.

Prerequisites

- Você pode copiar todos os snapshots acessíveis que tenham o status `completed`, incluindo snapshots compartilhados e snapshots que você criou.
- Você pode copiar snapshots do AWS Marketplace , do VM Import/Export e do AWS Storage Gateway, mas deve verificar se o snapshot é compatível com a Região de destino.

Considerations

- Cada conta pode ter até vinte solicitações simultâneas de cópia de snapshot para uma única região de destino.
- Tags definidas pelo usuário não são copiadas do snapshot de origem para o novo snapshot. É possível adicionar tags definidas pelo usuário durante ou depois da operação de cópia. Para obter mais informações, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).
- Os snapshots criados por uma operação de cópia de snapshot têm um ID arbitrário de volume que não deve ser usado para qualquer outra finalidade.
- As permissões de nível de recurso especificadas para a operação de cópia de snapshot se aplicam somente ao novo snapshot. Você não pode especificar permissões no nível do recurso para o snapshot de origem. Para ver um exemplo, consulte [Exemplo: Copiar snapshots \(p. 1160\)](#).

Pricing

- Para obter informações sobre definição de preços para cópias de snapshots entre regiões e contas da AWS, consulte [Definição de preço do Amazon EBS](#).
- Observe que as operações de cópia de snapshots em uma única conta e região não copiam dados reais e, portanto, são gratuitas, contanto que o status de criptografia da cópia do snapshot não seja alterado.
- Se você copiar um snapshot e criptografiá-lo com uma nova chave do KMS, será criada uma cópia completa (não incremental). Isso resulta em custos adicionais de armazenamento.
- Se você copiar um snapshot para uma nova região, será criada uma cópia completa (não incremental). Isso resulta em custos adicionais de armazenamento. Cópias subsequentes do mesmo snapshot são incrementais.

Cópias incrementais de snapshot

A determinação de se uma cópia do snapshot deve ser incremental é feita pela cópia do snapshot concluída mais recentemente. Ao copiar um snapshot entre regiões ou contas, a cópia será uma cópia incremental se as seguintes condições forem atendidas:

- O snapshot foi copiado anteriormente na conta ou região de destino.
- A cópia mais recente do snapshot ainda existe na conta ou região de destino.

- Todas as cópias do snapshot na conta ou região de destino foram feitas sem criptografia ou foram criptografadas usando a mesma chave do KMS.

Se a cópia mais recente do snapshot tiver sido excluída, a próxima cópia será um cópia completa, não uma cópia incremental. Se uma cópia ainda estiver pendente quando outra cópia for iniciada, esta será iniciada somente após a primeira cópia ser concluída.

Recomendamos marcar seus snapshots com o ID do volume e a hora da criação para que você possa manter o controle da cópia do snapshot mais recente de um volume na conta ou região de destino.

Para ver se as cópias dos snapshots são incrementais, verifique o evento [copySnapshot \(p. 1485\)](#) do CloudWatch

Cópia de snapshot e criptografia

Quando você copiar um snapshot, poderá criptografar a cópia ou especificar uma chave do KMS diferente da original, e o snapshot copiado resultante usará a nova chave do KMS. Contudo, a alteração do status de criptografia de um snapshot durante uma operação de cópia resulta em uma cópia (não incremental) completa, o que pode aumentar as cobranças de transferência e armazenamento de dados.

Para copiar um snapshot criptografado compartilhado de outra conta da AWS, você deve ter permissões para usar o snapshot e a chave mestra do cliente (CMK) que foi usada para criptografar o snapshot. Ao usar um snapshot criptografado que foi compartilhado com você, recomendamos que você refaça a criptografia do snapshot copiando-o por meio de uma chave do KMS própria. Isso protegerá você se a chave do KMS original estiver comprometida ou se o proprietário revogá-la, o que poderá fazer com que você perca o acesso aos volumes criptografados criados usando o snapshot. Para obter mais informações, consulte [Compartilhar um snapshot do Amazon EBS \(p. 1323\)](#).

Você aplica a criptografia a cópias de snapshots do EBS definindo o parâmetro `Encrypted` como `true`. (O parâmetro `Encrypted` é opcional se a opção [encryption by default \(p. 1426\)](#) (criptografia por padrão) estiver ativada).

Opcionalmente, você pode usar `KmsKeyId` para especificar uma chave personalizada para criptografar a cópia do snapshot. (O parâmetro `Encrypted` também deve ser definido como `true`, mesmo que a criptografia por padrão esteja ativada.) Se o parâmetro `KmsKeyId` não for especificado, a chave usada para a criptografia dependerá do estado de criptografia do snapshot de origem e de sua propriedade.

As tabelas a seguir descrevem o resultado da criptografia para cada combinação possível de configurações.

Tópicos

- [Resultados de criptografia: copiar snapshots de sua propriedade \(p. 1319\)](#)
- [Resultados de criptografia: copiar snapshots compartilhados com você \(p. 1320\)](#)

[Resultados de criptografia: copiar snapshots de sua propriedade](#)

Criptografia por padrão	O parâmetro <code>Encrypted</code> está definido?	Status de criptografia do snapshot de origem	Padrão (nenhuma chave do KMS especificada)	Personalizado (chave do KMS especificada)
Desabilitado	Não	Não criptografado	Não criptografado	N/D
		Criptografado	Criptografado por Chave gerenciada pela AWS	

Criptografia por padrão	O parâmetro Encrypted está definido?	Status de criptografia do snapshot de origem	Padrão (nenhuma chave do KMS especificada)	Personalizado (chave do KMS especificada)
	Sim	Não criptografado	Criptografado pela chave do KMS padrão	Criptografado pela chave do KMS especificada**
		Criptografado	Criptografado pela chave do KMS padrão	
Enabled	Não	Não criptografado	Criptografado pela chave do KMS padrão	N/D
		Criptografado	Criptografado pela chave do KMS padrão	
	Sim	Não criptografado	Criptografado pela chave do KMS padrão	Criptografado pela chave do KMS especificada**
		Criptografado	Criptografado pela chave do KMS padrão	

** Essa é uma chave gerenciada pelo cliente especificada para a ação de cópia. Essa chave gerenciada pelo cliente é usada em vez da chave gerenciada pelo cliente padrão para a conta e a região da AWS.

Resultados de criptografia: copiar snapshots compartilhados com você

Criptografia por padrão	O parâmetro Encrypted está definido?	Status de criptografia do snapshot de origem	Padrão (nenhum KmsKeyId especificado)	Personalizado (KmsKeyId especificado)
Desabilitado	Não	Não criptografado	Não criptografado	N/D
		Criptografado	Criptografado por Chave gerenciada pela AWS	
	Sim	Não criptografado	Criptografado pela chave do KMS padrão	Criptografado pela chave do KMS especificada**
		Criptografado	Criptografado pela chave do KMS padrão	
Enabled	Não	Não criptografado	Criptografado pela chave do KMS padrão	N/D

Criptografia por padrão	O parâmetro Encrypted está definido?	Status de criptografia do snapshot de origem	Padrão (nenhum KmsKeyId especificado)	Personalizado (KmsKeyId especificado)
	Sim	Criptografado	Criptografado pela chave do KMS padrão	Criptografado pela chave do KMS especificada**
		Não criptografado	Criptografado pela chave do KMS padrão	
		Criptografado	Criptografado pela chave do KMS padrão	

** Essa é uma chave gerenciada pelo cliente especificada para a ação de cópia. Essa chave gerenciada pelo cliente é usada em vez da chave gerenciada pelo cliente padrão para a conta e a região da AWS.

Copiar um snapshot

Para copiar um snapshot, use um dos métodos a seguir.

Console

Para copiar um snapshot usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot a ser copiado e escolha em Copiar na lista Ações.
4. Na caixa de diálogo Copiar snapshot, atualize o seguinte conforme necessário:
 - Região de destino: selecione a região onde você deseja gravar a cópia do snapshot.
 - Descrição: Por padrão, descrição inclui informações sobre o snapshot de origem, de forma que você possa identificar uma cópia do original. Você pode alterar essa descrição conforme necessário.
 - Criptografia: Se o snapshot de origem não for criptografado, você poderá optar por criptografar a cópia. Se você tiver habilitado a [criptografia por padrão](#) (p. 1426), a opção Encryption (Criptografia) será configurada e não poderá ser desconfigurada no console do snapshot. Se a opção Encryption (Criptografia) estiver configurada, você poderá escolher criptografá-la para uma CMK gerenciada pelo cliente ao selecionar uma no campo, conforme descrito abaixo.

Você não pode remover a criptografia de um snapshot criptografado.

- Master Key (Chave mestra): a chave mestra (CMK) do cliente que deve ser usada para criptografar esse snapshot. A chave padrão da sua conta é exibida inicialmente, mas você pode selecioná-la nas chaves mestras da sua conta ou digitar/colar o ARN de uma chave de uma conta diferente. Você pode criar novas chaves mestras de criptografia no [console do AWS KMS](#).
5. Escolha Copiar.
 6. Na caixa de diálogo de confirmação Copy Snapshot (Copiar snapshot), escolha Snapshots para acessar a página Snapshots na região especificada ou escolha Close (Fechar).

Para visualizar o andamento do processo de cópia, troque para a região de destino e atualize a página Snapshots. As cópias em andamento estão listadas na parte superior da página.

AWS CLI

Para copiar um snapshot usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [copy-snapshot \(AWS CLI\)](#)
- [Copy-EC2Snapshot \(AWS Tools for Windows PowerShell\)](#)

Para verificar se há falhas

Se você tentar copiar um snapshot criptografado sem ter permissão para usar a chave de criptografia, a operação falhará silenciosamente. O estado de erro não é exibido no console até você atualizar a página. Você também pode verificar o estado do snapshot a partir da linha de comando, conforme o exemplo a seguir.

```
aws ec2 describe-snapshots --snapshot-id snap-0123abcd
```

Se uma cópia falhar por conta de permissões de chaves insuficientes, você verá a seguinte mensagem: "StateMessage": "O ID da chave apresentada não pode ser acessado".

Para copiar um snapshot criptografado, você deve ter as permissões `DescribeKey` no CMK padrão. Negar explicitamente essas permissões resulta em falha da cópia. Para obter informações sobre o gerenciamento das chaves de CMK, consulte [Controle de acesso às chaves mestras do cliente](#).

Exibir informações do snapshot do Amazon EBS

Você pode visualizar informações detalhadas sobre seus snapshots usando um dos métodos a seguir.

Console

Para visualizar informações de snapshots usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione Snapshots no painel de navegação.
3. Para reduzir a lista, escolha uma opção na lista Filtro. Por exemplo, para exibir somente os snapshots, escolha De minha propriedade. Você também pode filtrar seus snapshots usando tags e atributos de snapshot. Escolha a barra de pesquisa para exibir as tags e atributos disponíveis.
4. Para ver mais informações sobre um snapshot, selecione-o.

AWS CLI

Para visualizar informações de snapshots usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [describe-snapshots \(AWS CLI\)](#)
- [Get-EC2Snapshot \(AWS Tools for Windows PowerShell\)](#)

Example Exemplo 1: filtro baseado em tags

O comando a seguir descreve os snapshots com a tag `Stack=production`.

```
aws ec2 describe-snapshots --filters Name=tag:Stack,Values=production
```

Example Exemplo 2: filtro baseado em volume

O comando a seguir descreve os snapshots criados do volume especificado.

```
aws ec2 describe-snapshots --filters Name=volume-id,Values=vol-049df61146c4d7901
```

Example Exemplo 3: filtro baseado na idade do snapshot

Com a AWS CLI, você pode usar JMESPath para filtrar resultados usando expressões. Por exemplo, o comando a seguir exibe os IDs de todos os snapshots criados pela sua conta da AWS (representada por **123456789012**) antes da data especificada (representada por **31/03/2020**). Se você não especificar o proprietário, os resultados incluirão todos os snapshots públicos.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?(StartTime<=`2020-03-31`)].[SnapshotId]" --output text
```

O comando a seguir exibe os IDs de todos os snapshots criados no intervalo de datas especificado.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?(StartTime>=`2019-01-01` && (StartTime<=`2019-12-31`)].[SnapshotId]" --output text
```

Compartilhar um snapshot do Amazon EBS

É possível modificar as permissões de um snapshot se você quiser compartilhá-lo com outras contas da AWS. Você pode compartilhar snapshots publicamente com todas as outras contas da AWS, ou você pode compartilhá-las de forma privada com as contas da AWS que você especificar. Os usuários autorizados por você poderão usar os snapshots que você compartilhar para criar os próprios volumes do EBS, ao passo que seu snapshot original não será afetado.

Important

Ao compartilhar um snapshot, você está oferecendo a outras pessoas o acesso a todos os dados no snapshot. Compartilhe snapshots somente com as pessoas de sua confiança com todos os dados do snapshot.

Tópicos

- [Antes de compartilhar um snapshot \(p. 1323\)](#)
- [Compartilhar um snapshot \(p. 1324\)](#)
- [Compartilhar uma chave do KMS \(p. 1325\)](#)
- [Exibir snapshots que são compartilhados com você \(p. 1326\)](#)
- [Usar snapshots que são compartilhados com você \(p. 1327\)](#)
- [Determinar o uso de snapshots compartilhados por você \(p. 1327\)](#)

Antes de compartilhar um snapshot

As seguintes considerações se aplicam ao compartilhamento de snapshots:

- Os snapshots são restritos à região na qual foram criados. Para compartilhar um snapshot com outra região, copie o snapshot nessa região e, em seguida, compartilhe a cópia. Para obter mais informações, consulte [Copiar um snapshot do Amazon EBS. \(p. 1317\)](#).

- Não é possível compartilhar snapshots criptografados com a Chave gerenciada pela AWS padrão. Você só pode compartilhar snapshots criptografados com uma chave gerenciada pelo cliente. Para obter mais informações, consulte [Creating keys](#) (Criar chaves) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).
- Você pode compartilhar apenas snapshots não criptografados publicamente.
- Ao compartilhar um snapshot criptografado, também é necessário compartilhar a chave gerenciada pelo cliente usada para criptografar o snapshot. Para obter mais informações, consulte [Compartilhar uma chave do KMS](#) (p. 1325).

Compartilhar um snapshot

É possível compartilhar um snapshot usando um dos métodos descritos na seção.

Console

Para compartilhar um snapshot

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione Snapshots no painel de navegação.
3. Selecione o snapshot e, em seguida, escolha Actions (Ações), Modify Permissions (Modificar permissões).
4. Para tornar o snapshot público ou compartilhá-lo com contas específicas da AWS, faça o seguinte:
 - Para tornar o snapshot público, escolha Público.
 - Para compartilhar o snapshot com uma ou mais contas da AWS, escolha Private (Privado), insira o ID da conta da AWS (sem hífen) em AWSAccount Number (Número da conta da AWS) e escolha Add Permission (Adicionar permissão). Repita a ação para as contas adicionais da AWS.
5. Escolha Save (Salvar).

AWS CLI

As permissões de um snapshot são especificadas usando o atributo `createVolumePermission` do snapshot. Para tornar um snapshot público, defina o grupo como `all`. Para compartilhar um snapshot com uma conta da AWS específica, defina o usuário como o ID da conta da AWS.

Para compartilhar um snapshot publicamente

Use um dos seguintes comandos.

- [modify-snapshot-attribute](#) (AWS CLI)

Para `--attribute`, especifique `createVolumePermission`. Para `--operation-type`, especifique `add`. Para `--group-names`, especifique `all`.

```
$ aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute createVolumePermission --operation-type add --group-names all
```

- [Edit-EC2SnapshotAttribute](#) (AWS Tools for Windows PowerShell)

Para `-Attribute`, especifique `CreateVolumePermission`. Para `-OperationType`, especifique `Add`. Para `-GroupName`, especifique `all`.

```
PS C:\> Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute CreateVolumePermission -OperationType Add -GroupName all
```

Para compartilhar um snapshot de forma privada

Use um dos seguintes comandos.

- [modify-snapshot-attribute \(AWS CLI\)](#)

Para --attribute, especifique `createVolumePermission`. Para --operation-type, especifique `add`. Para --user-ids, especifique os IDs de 12 dígitos da propriedade das contas da AWS com as quais os snapshots serão compartilhados.

```
$ aws ec2 modify-snapshot-attribute --snapshot-id 1234567890abcdef0 --attribute createVolumePermission --operation-type add --user-ids 123456789012
```

- [Edit-EC2SnapshotAttribute \(AWS Tools for Windows PowerShell\)](#)

Para `-Attribute`, especifique `CreateVolumePermission`. Para `-OperationType`, especifique `Add`. Para `UserId`, especifique os IDs de 12 dígitos da propriedade das contas da AWS com as quais os snapshots serão compartilhados.

```
PS C:\> Edit-EC2SnapshotAttribute -SnapshotId 1234567890abcdef0 -Attribute CreateVolumePermission -OperationType Add -UserId 123456789012
```

Compartilhar uma chave do KMS

Ao compartilhar um snapshot criptografado, também é necessário compartilhar a chave gerenciada pelo cliente usada para criptografar o snapshot. Você pode aplicar permissões entre contas a uma chave gerenciada pelo cliente quando ela é criada ou posteriormente.

Os usuários da sua chave gerenciada pelo cliente compartilhada que estão acessando snapshots criptografados devem receber permissões para executar as seguintes ações na chave:

- `kms:DescribeKey`
- `kms>CreateGrant`
- `kms:GenerateDataKey`
- `kms:ReEncrypt`
- `kms:Decrypt`

Para obter mais informações sobre como controlar o acesso a uma chave gerenciada pelo cliente, consulte [Using key policies in AWS KMS](#) (Usar políticas de chaves no AWS Key Management Service) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

Para compartilhar a chave gerenciada pelo cliente usando o console do AWS KMS

1. Abra o console do AWS KMS em <https://console.aws.amazon.com/kms>.
2. Para alterar a região da AWS, use o Region selector (Seletor de regiões) no canto superior direito da página.
3. No painel de navegação, escolha Customer managed keys (Chaves gerenciadas pelo cliente).
4. Na coluna Alias, escolha o alias (link de texto) da chave gerenciada pelo cliente usada para criptografar o snapshot. Os principais detalhes são abertos em uma nova página.
5. Na seção Key policy (Política de chave), você verá a exibição de política ou a exibição padrão. A exibição de política exibe o documento de política de chaves. A exibição padrão exibe seções para Key administrators (Administradores de chave), Key deletion (Exclusão de chave), Key Use (Uso de chave) e Other AWS accounts (Outras contas da AWS). A exibição padrão é exibida se você criou a

política no console e não a personalizou. Se a exibição padrão não estiver disponível, será necessário editar manualmente a política na exibição de política. Para obter mais informações, consulte [Viewing a key policy \(console\)](#) (Exibir uma política de chave (console)) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

Use a exibição de políticas ou a exibição padrão, dependendo da exibição que você pode acessar, para adicionar um ou mais IDs de conta da AWS à política, da seguinte forma:

- (Exibição de política) Escolha Edit (Editar). Adicione um ou mais IDs de conta da AWS às seguintes instruções: "Allow use of the key" e "Allow attachment of persistent resources". Selecione Save changes (Salvar alterações). No exemplo a seguir, o ID da conta da AWS 444455556666 é adicionado à política.

```
{  
    "Sid": "Allow use of the key",  
    "Effect": "Allow",  
    "Principal": {"AWS": [  
        "arn:aws:iam::111122223333:user/KeyUser",  
        "arn:aws:iam::444455556666:root"  
    ]},  
    "Action": [  
        "kms:Encrypt",  
        "kms:Decrypt",  
        "kms:ReEncrypt*",  
        "kms:GenerateDataKey*",  
        "kms:DescribeKey"  
    ],  
    "Resource": "*"  
},  
{  
    "Sid": "Allow attachment of persistent resources",  
    "Effect": "Allow",  
    "Principal": {"AWS": [  
        "arn:aws:iam::111122223333:user/KeyUser",  
        "arn:aws:iam::444455556666:root"  
    ]},  
    "Action": [  
        "kms>CreateGrant",  
        "kms>ListGrants",  
        "kms:RevokeGrant"  
    ],  
    "Resource": "*",  
    "Condition": {"Bool": {"kms:GrantIsForAWSResource": true}}  
}
```

- (Exibição padrão) Role para baixo até Other AWS accounts (Outras contas da AWS). Escolha Add other AWS accounts (Adicionar outras contas da AWS) e insira o ID da conta da AWS conforme solicitado. Para adicionar outra conta, escolha Add another AWS account (Adicionar outra conta da AWS) e insira o ID da conta da AWS. Depois de adicionar todas as contas da AWS, escolha Save changes (Salvar alterações).

Exibir snapshots que são compartilhados com você

Use um dos métodos a seguir para exibir snapshots compartilhados com você.

Console

Para exibir snapshots compartilhados usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Snapshots.

3. Filtre os instantâneos listados. No canto superior esquerdo da tela, escolha uma das seguintes opções:

- Snapshots privados: para visualizar somente snapshots compartilhados com você de forma privada.
- Snapshots públicos: para visualizar somente snapshots compartilhados com você publicamente.

AWS CLI

Para visualizar permissões de snapshots usando a linha de comando

Use um dos seguintes comandos:

- [describe-snapshot-attribute](#) (AWS CLI)
- [Get-EC2SnapshotAttribute](#) (AWS Tools for Windows PowerShell)

Usar snapshots que são compartilhados com você

Para usar um snapshot compartilhado não criptografado

Localize o snapshot compartilhado pelo ID ou pela descrição. Para obter mais informações, consulte [Exibir snapshots que são compartilhados com você \(p. 1326\)](#). Você pode usar esse instantâneo como faria com qualquer outro snapshot que você tenha na sua conta. Por exemplo, você pode criar um volume do snapshot ou copiá-lo para outra região.

Para usar um snapshot criptografado compartilhado

Localize o snapshot compartilhado pelo ID ou pela descrição. Para obter mais informações, consulte [Exibir snapshots que são compartilhados com você \(p. 1326\)](#). Crie uma cópia do snapshot compartilhado em sua conta e criptografe-a com uma chave do KMS de sua propriedade. Em seguida, você pode usar a cópia para criar volumes ou copiá-la para regiões diferentes.

Determinar o uso de snapshots compartilhados por você

É possível usar o AWS CloudTrail para monitorar se um snapshot que você compartilhou com outras pessoas foi copiado ou usado para criar um volume. Os seguintes eventos são registrados em log no CloudTrail:

- SharedSnapshotCopyInitiated: um snapshot compartilhado está sendo copiado.
- SharedSnapshotVolumeCreated: um snapshot compartilhado está sendo usado para criar um volume.

Para obter mais informações sobre o uso de CloudTrail, consulte [Registrar em log o Amazon EC2 e chamadas de APIs do Amazon EBS com o AWS CloudTrail \(p. 937\)](#).

Amazon EBS local snapshots on Outposts

Os snapshots do Amazon EBS são uma cópia point-in-time dos volumes do EBS.

Por padrão, os snapshots de volumes do EBS em um Outpost são armazenados no Amazon S3, na região do Outpost. Você também pode usar Snapshots locais do Amazon EBS em Outposts para armazenar snapshots de volumes em um Outpost localmente no Amazon S3 no próprio Outpost. Isso garante que os dados do snapshot permaneçam no Outpost e no seu local. Além disso, você pode usar políticas e permissões do AWS Identity and Access Management (IAM) para configurar políticas de imposição de residência de dados para garantir que os dados de snapshots não saiam do Outpost. Isso é especialmente

útil se você mora em um país ou região que ainda não foi atendida por uma região da AWS e que apresente requisitos de residência de dados.

Este tópico fornece informações sobre como trabalhar com Snapshots locais do Amazon EBS em Outposts. Para obter mais informações sobre os snapshots do Amazon EBS e sobre como trabalhar com snapshots em uma região da AWS, consulte [Snapshots do Amazon EBS \(p. 1294\)](#).

Para obter mais informações sobre AWS Outposts, consulte [AWS Outposts Features \(Recursos\)](#) e o [AWS Outposts Guia do Usuário](#). Para obter informações sobre preços, consulte [Preços do AWS Outposts](#).

Tópicos

- [Perguntas frequentes \(p. 1328\)](#)
- [Prerequisites \(p. 703\)](#)
- [Considerations \(p. 252\)](#)
- [Controlar o acesso com o IAM \(p. 1330\)](#)
- [Trabalhe com snapshots locais \(p. 1331\)](#)

Perguntas frequentes

1. O que são snapshots locais?

Por padrão, os snapshots de volumes do Amazon EBS em um Outpost são armazenados no Amazon S3, na região do Outpost. Se o Outpost estiver provisionado com o Amazon S3 on Outposts, você pode optar por armazenar os snapshots localmente no próprio Outpost. Os snapshots locais são incrementais, o que significa que serão salvos somente os blocos no volume que mudaram após o snapshot mais recente. Você pode usar esses snapshots para restaurar a qualquer momento um volume no mesmo Outpost que o snapshot. Para obter mais informações sobre snapshots do Amazon EBS, consulte [Snapshots do Amazon EBS \(p. 1294\)](#).

2. Por que devo usar snapshots locais?

Os snapshots são uma maneira conveniente de fazer backup de seus dados. Com snapshots locais, todos os seus dados de snapshots são armazenados localmente no Outpost. Isso significa que ele não deixa o seu local. Isso será útil principalmente se você mora em um país ou região que ainda não está atendida por uma região da AWS e que apresente requisitos de residência.

Além disso, o uso de snapshots locais pode ajudar a reduzir a largura de banda usada para a comunicação entre a Região e o Outpost em ambientes restritos pela largura de banda.

3. Como faço para impor a residência de dados de snapshots em Outposts?

Você pode usar políticas do AWS Identity and Access Management (IAM) para controlar as permissões que os principais (contas da AWS, usuários do IAM e funções do IAM) têm ao trabalhar com snapshots locais para impor a residência de dados. Você pode criar uma política que evite que as entidades criem snapshots a partir de volumes e instâncias do Outpost e armazenem os snapshots em uma região da AWS. No momento, não há suporte para copiar snapshots e imagens de um Outpost para uma região. Para obter mais informações, consulte [Controlar o acesso com o IAM \(p. 1330\)](#).

4. Há suporte para snapshots locais multivolume e consistentes com falhas?

Sim, você pode criar snapshots locais multivolume e consistentes com falhas em instâncias em um Outpost.

5. Como crio snapshots locais?

Você pode criar snapshots manualmente usando a AWS Command Line Interface (AWS CLI) ou o console do Amazon EC2. Para obter mais informações, consulte, [Trabalhe com snapshots locais \(p. 1331\)](#). Você também pode automatizar o ciclo de vida de snapshots locais por meio do Amazon Data Lifecycle Manager. Para obter mais informações, consulte, [Automatize snapshots em um Outpost \(p. 1337\)](#).

6. Posso criar, usar ou excluir snapshots locais se meu Outpost perder a conectividade com a sua região?

Não. O Outpost deve ter conectividade com a região dele, pois ela fornece serviços de acesso, autorização, registro em log e monitoramento, que são essenciais para a integridade de seus snapshots. Se não houver conectividade, você não poderá criar novos snapshots locais, criar volumes, executar instâncias a partir de snapshots locais existentes ou excluir snapshots locais.

7. O quanto rápido a capacidade de armazenamento do Amazon S3 fica disponível após a exclusão de snapshots locais?

A capacidade de armazenamento do Amazon S3 fica disponível dentro de 72 horas após a exclusão de snapshots locais e de volumes que fazem referência a eles.

8. Como posso garantir que a capacidade do Amazon S3 não se esgote no meu Outpost?

Recomendamos que você use alarmes Amazon CloudWatch para monitorar a sua capacidade de armazenamento do Amazon S3 e exclua snapshots e volumes de que não precisa mais; assim você previne o fim da capacidade de armazenamento. Se você estiver usando o Amazon Data Lifecycle Manager para automatizar o ciclo de vida de snapshots locais, certifique-se de que as suas políticas de retenção de snapshots não retenham snapshots por mais tempo do que o necessário.

9. Posso usar snapshots locais e AMIs baseadas em snapshots locais com instâncias spot e uma frota spot?

Não, você não pode usar snapshots locais ou AMIs baseadas em snapshots locais para executar instâncias spot ou uma frota spot.

10. Posso usar snapshots locais e AMIs baseadas em snapshots locais com o Amazon EC2 Auto Scaling?

Sim, você pode usar snapshots locais e AMIs baseadas em snapshots locais para iniciar grupos de Auto Scaling em uma sub-rede que esteja no mesmo Outpost que os snapshots. A função vinculada a serviços do grupo Amazon EC2 Auto Scaling deve ter permissão para usar a Chave do KMS usada para criptografar os snapshots.

Você não pode usar snapshots locais ou AMIs compatíveis com snapshots locais para iniciar grupos do Auto Scaling em uma região da AWS.

Prerequisites

Para armazenar snapshots em um Outpost, você deve ter um Outpost provisionado com o Amazon S3 em Outposts. Para obter mais informações sobre o Amazon S3 em Outposts, consulte [Using Amazon S3 on Outposts](#) (Usar o S3 em Outposts) no Guia do desenvolvedor do Amazon Simple Storage Service.

Considerations

Ao trabalhar com snapshots locais, lembre-se do seguinte:

- O Outpost deve ter conectividade em sua região da AWS para usar snapshots locais.
- Os metadados do snapshot são armazenados na região da AWS associada ao Outpost. Isso não inclui nenhum dado de snapshot.
- Os snapshots armazenados em Outposts são criptografados por padrão. Não há suporte para snapshots não criptografados. Os snapshots criados em um Outpost e snapshots copiados para um Outpost são criptografados usando a Chave do KMS de criptografia padrão para a região ou uma Chave do KMS diferente que você especificar ao fazer a solicitação.
- Ao criar um volume em um Outpost a partir de um snapshot local, você não pode criptografar o volume novamente usando uma Chave do KMS de criptografia diferente. Os volumes criados de snapshots locais devem ser criptografados usando a mesma Chave do KMS que o snapshot de origem.
- Depois que você excluir snapshots locais de um Outpost, a capacidade de armazenamento do Amazon S3 usada pelos snapshots excluídos fica disponível por 72 horas. Para obter mais informações, consulte [Exclua snapshots locais \(p. 1336\)](#).

- Você não pode exportar snapshots locais de um Outpost.
- Você não pode habilitar a restauração rápida de snapshots para snapshots locais.
- APIs diretas do EBS não são compatíveis com snapshots locais.
- Não é possível copiar snapshots locais ou AMIs de um Outpost para uma região da AWS, de um Outpost para outro ou dentro de um Outpost. No entanto, você pode copiar snapshots de uma região da AWS para um Outpost. Para obter mais informações, consulte [Copiar snapshots de uma região da AWS para um Outpost \(p. 1335\)](#).
- Ao copiar um snapshot de uma região da AWS para um Outpost, os dados são transferidos pelo link de serviço. Copiar vários snapshots simultaneamente pode afetar outros serviços em execução no Outpost.
- Você não pode compartilhar snapshots locais.
- Você deve usar as políticas do IAM para garantir que seus requisitos de residência de dados sejam cumpridos. Para obter mais informações, consulte [Controlar o acesso com o IAM \(p. 1330\)](#).
- Os Snapshots locais são backups incrementais. Serão salvos somente os blocos no volume que foram alterados depois do seu snapshot mais recente. Cada snapshot local contém todas as informações necessárias para restaurar os seus dados (desde o momento em que o snapshot foi capturado) até um volume novo do EBS. Para obter mais informações, consulte [Como funcionam os snapshots incrementais \(p. 1295\)](#).
- Você não pode usar políticas do IAM para impor a residência de dados para as ações CopySnapshot (Copiar snapshot) e CopyImage (Copiar imagem).

Controlar o acesso com o IAM

Você pode usar políticas do AWS Identity and Access Management (IAM) para controlar as permissões que os principais (contas da AWS, usuários do IAM e funções do IAM) têm ao trabalhar com snapshots locais. Veja a seguir as políticas de exemplo que você pode usar para conceder ou negar permissão para executar ações específicas com snapshots locais.

Important

No momento, não há suporte para copiar snapshots e imagens de um Outpost para uma região. Como resultado, você não pode usar as políticas do IAM para impor a residência de dados para as ações CopySnapshot (Copiar snapshot) e CopyImage (Copiar imagem).

Tópicos

- [Imponha a residência de dados para snapshots \(p. 1330\)](#)
- [Impeça que as entidades excluam snapshots locais \(p. 1331\)](#)

Imponha a residência de dados para snapshots

A política de exemplo a seguir impede que todas as entidades criem snapshots de volumes e instâncias no Outpost arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef e armazenem os dados de snapshot em uma região da AWS. As entidades ainda podem criar snapshots locais. Essa política garante que todos os snapshots permaneçam no Outpost.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": [  
                "ec2:CreateSnapshot",  
                "ec2:CreateSnapshots"  
            ],  
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",  
            "Condition": {  
                "StringEquals": {  
                    "aws:outpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef"  
                }  
            }  
        }  
    ]  
}
```

```
        "ec2:SourceOutpostArn": "arn:aws:outposts:us-
east-1:123456789012:outpost/op-1234567890abcdef0"
    },
    "Null": {
        "ec2:OutpostArn": "true"
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateSnapshot",
        "ec2:CreateSnapshots"
    ],
    "Resource": "*"
}
]
```

Impêça que as entidades excluam snapshots locais

A política de exemplo a seguir impede que todos as entidades excluam snapshots locais armazenados no Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "arn:aws:ec2:us-east-1::snapshot/*",
            "Condition": {
                "StringEquals": {
                    "ec2:OutpostArn": "arn:aws:outposts:us-east-1:123456789012:outpost/
op-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot"
            ],
            "Resource": "*"
        }
    ]
}
```

Trabalhe com snapshots locais

As seções a seguir explicam como usar snapshots locais.

Tópicos

- [Regras para armazenar snapshots \(p. 1332\)](#)
- [Crie snapshots locais a partir de volumes em um Outpost \(p. 1332\)](#)
- [Crie snapshots locais multivolume a partir de instâncias em um Outpost \(p. 1333\)](#)
- [Crie AMIs em snapshots locais \(p. 1334\)](#)
- [Copiar snapshots de uma região da AWS para um Outpost \(p. 1335\)](#)
- [Copiar AMIs de uma região da AWS para um Outpost \(p. 1336\)](#)

- [Crie volumes a partir de snapshots locais \(p. 1336\)](#)
- [Execute instâncias a partir de AMIs baseadas em snapshots locais \(p. 1336\)](#)
- [Exclua snapshots locais \(p. 1336\)](#)
- [Automatize snapshots em um Outpost \(p. 1337\)](#)

Regras para armazenar snapshots

As regras a seguir se aplicam ao armazenamento de snapshots:

- Se o snapshot mais recente de um volume for armazenado em um Outpost, todos os snapshots sucessivos deverão ser armazenados no mesmo Outpost.
- Se o snapshot mais recente de um volume for armazenado em uma região da AWS, todos os snapshots sucessivos deverão ser armazenados na mesma região. Para começar a criar snapshots locais a partir desse volume, faça o seguinte:
 1. Crie um snapshot do volume na região da AWS.
 2. Copie o snapshot para o Outpost da região da AWS.
 3. Crie um novo volume a partir do snapshot local.
 4. Anexe o volume a uma instância no Outpost.

Para o novo volume no Outpost, o próximo snapshot pode ser armazenado no Outpost ou na região da AWS. Todos os snapshots sucessivos deverão ser armazenados nessa mesma localização.

- Os snapshots locais, incluindo snapshots criados em um Outpost e snapshots copiados para um Outpost de uma região da AWS, só podem ser usados para criar volumes no mesmo Outpost.
- Se você criar um volume em um Outpost a partir de um snapshot em uma região, todos os snapshots sucessivos desse novo volume deverão ficar na mesma região.
- Se você criar um volume em um Outpost de um snapshot local, todos os snapshots sucessivos desse novo volume deverão estar no mesmo Outpost.

Crie snapshots locais a partir de volumes em um Outpost

Você pode criar snapshots locais a partir de volumes no seu Outpost. Você pode optar por armazenar os snapshots no mesmo Outpost que o volume de origem ou na região do Outpost.

Os Snapshots locais podem ser usados para criar volumes somente no mesmo Outpost.

Você pode criar snapshots locais a partir de volumes em um Outpost usando um dos métodos a seguir.

Console

Para criar snapshots locais a partir de volumes em um Outpost

Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

1. No painel de navegação, escolha Volumes.
2. Selecione o volume no Outpost e escolha Actions (Ações) e Create snapshot (Criar snapshot).
3. (Opcional) Em Description (Descrição), insira uma breve descrição para o snapshot.
4. Em Snapshot destination Destino do snapshot), escolha AWS Outpost. O snapshot será criado no mesmo Outpost que o volume de origem. O campo Outpost ARN (ARN do Outpost) exibe o nome de recurso da Amazon (ARN) do Outpost de destino.
5. (Opcional) Escolha Add Tag (Adicionar tag) para adicionar tags ao seu snapshot. Para cada tag, forneça uma chave e um valor.
6. Escolha Create Snapshot (Criar snapshot).

Command line

Para criar snapshots locais a partir de volumes em um Outpost

Use o comando `create-snapshot` (Criar snapshot). Especifique o ID do volume a partir do qual deseja criar o snapshot e o ARN do Outpost de destino em que deseja armazenar o snapshot. Se você omitir o ARN do Outpost, o snapshot será armazenado na região da AWS do Outpost.

Por exemplo, o comando a seguir cria um snapshot local de volume `vol-1234567890abcdef0` e armazena o snapshot no Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 create-snapshot --volume-id vol-1234567890abcdef0 --outpost-arn arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0 --description "single volume local snapshot"
```

Crie snapshots locais multivolume a partir de instâncias em um Outpost

Você pode criar snapshots locais multivolume e consistentes com falhas em instâncias no seu Outpost. Você pode optar por armazenar os snapshots no mesmo Outpost que a instância de origem ou na região do Outpost.

Os snapshots locais multivolume podem ser usados para criar volumes somente no mesmo Outpost.

Você pode criar snapshots locais multivolume a partir de instâncias em um Outpost usando um dos métodos a seguir.

Console

Para criar snapshots locais multivolume a partir de instâncias em um Outpost

Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

1. No painel de navegação, selecione Snapshots.
2. Escolha Create Snapshot (Criar snapshot).
3. Em Select resource type (Selecionar tipo de recurso), escolha Instance (Instância).
4. Em Instance ID (ID de instância), selecione a instância no Outpost a partir da qual deseja criar os snapshots.
5. (Opcional) Em Description (Descrição), insira uma breve descrição para os snapshots.
6. Em Snapshot destination Destino do snapshot), escolha AWS Outpost. Os snapshots serão criados no mesmo Outpost que a instância de origem. O Outpost ARN (ARN do Outpost) exibe o ARN do Outpost de destino.
7. (Opcional) Para excluir o volume raiz e evitar que se torne um snapshot, selecione Exclude root volume (Excluir volume raiz).
8. (Opcional) Para copiar tags automaticamente do volume de origem para os snapshots, selecione Copy tags from volume (Copiar tags do volume). Isso define os metadados do snapshot, como políticas de acesso, informações de anexo e alocação de custos, para corresponderem com o volume de origem.
9. (Opcional) Escolha Add Tag (Adicionar tag) para adicionar tags ao seu snapshot. Para cada tag, forneça uma chave e um valor.
10. Escolha Create Snapshot (Criar snapshot).

Durante a criação do snapshot, os snapshots são gerenciados juntos. Se houver falha em um dos snapshots do conjunto de volumes, os outros snapshots no conjunto ficarão com o status de erro.

Command line

Para criar snapshots locais multivolume a partir de instâncias em um Outpost

Use o comando [create-snapshots](#) (Criar snapshots). Especifique o ID da instância a partir da qual deseja criar os snapshots e o ARN do Outpost de destino em que deseja armazenar os snapshots. Se você omitir o ARN do Outpost, os snapshots serão armazenados na região da AWS do Outpost.

Por exemplo, o comando a seguir cria snapshots dos volumes anexados à instância `i-1234567890abcdef0` e armazena os snapshots no Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 create-snapshots --instance-specification InstanceId=i-1234567890abcdef0 --outpost-arn arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0 --description "multi-volume local snapshots"
```

Crie AMIs em snapshots locais

Você pode criar Imagens de máquina da Amazon (AMIs) usando uma combinação de snapshots locais e snapshots armazenados na região do Outpost. Por exemplo, se tiver um Outpost na região `us-east-1`, você poderá criar uma AMI com volumes de dados que são baseados em snapshots locais nesse Outpost e um volume raiz que é baseado em um snapshot na região `us-east-1`.

Note

- Não é possível criar AMIs que incluam snapshots de base armazenados em vários Outposts.
- No momento, você não pode criar AMIs diretamente de instâncias em Outposts usando a API `CreateImage` (Criar imagem) ou o console do Amazon EC2 para Outposts habilitados ao Amazon S3 em Outposts.
- As AMIs baseadas em snapshots locais podem ser usadas para executar instâncias somente no mesmo Outpost.

Para criar uma AMI em um Outpost a partir de snapshots em uma região

1. Copie os snapshots da região para o Outpost. Para obter mais informações, consulte [Copiar snapshots de uma região da AWS para um Outpost \(p. 1335\)](#).
2. Use o console do Amazon EC2 ou o comando [register-image](#) (Registrar imagem) para criar a AMI usando as cópias de snapshots no Outpost. Para obter mais informações, consulte [Creating an AMI from a snapshot](#) (Como criar uma AMI a partir de um snapshot).

Para criar uma AMI em um Outpost a partir de uma instância em um Outpost

1. Crie snapshots a partir da instância no Outpost e armazene os snapshots no Outpost. Para obter mais informações, consulte [Crie snapshots locais multivolume a partir de instâncias em um Outpost \(p. 1333\)](#).
2. Use o console do Amazon EC2 ou o comando [register-image](#) (Registrar imagem) para criar a AMI usando os snapshots locais. Para obter mais informações, consulte [Creating an AMI from a snapshot](#) (Como criar uma AMI a partir de um snapshot).

Para criar uma AMI em uma região a partir de uma instância em um Outpost

1. Crie snapshots a partir da instância no Outpost e armazene-os na região. Para obter mais informações, consulte [Crie snapshots locais a partir de volumes em um Outpost \(p. 1332\)](#) ou [Crie snapshots locais multivolume a partir de instâncias em um Outpost \(p. 1333\)](#).

2. Use o console do Amazon EC2 ou o comando [register-image](#) para criar a AMI usando as cópias de snapshot na região. Para obter mais informações, consulte [Creating an AMI from a snapshot](#) (Como criar uma AMI a partir de um snapshot).

Copiar snapshots de uma região da AWS para um Outpost

Você pode copiar snapshots a partir de uma região da AWS para um Outpost. Você pode fazer isso somente se os snapshots estiverem na região do Outpost. Se os snapshots estiverem em uma região diferente, você deve copiar primeiro o snapshot para a região do Outpost e, em seguida, copiá-lo dessa região para o Outpost.

Note

Você não pode copiar snapshots locais de um Outpost para uma região, de um Outpost para outro ou dentro do mesmo Outpost.

Você pode copiar snapshots de uma região para um Outpost usando um dos métodos a seguir.

Console

Para copiar um snapshot de uma região da AWS para um Outpost

Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

1. No painel de navegação, selecione Snapshots.
2. Selecione o snapshot e escolha Actions (Ações) e Copy (Copiar).
3. Em Destination Region (Região de destino), escolha a região para o Outpost de destino.
4. Em Snapshot Destination (Destino do snapshot), escolha AWS Outpost.

O campo Snapshot Destination (Destino do snapshot) só será exibido se você tiver Outposts na região de destino selecionada. Se o campo não aparecer, você não terá nenhum Outpost na região de destino selecionada.

5. Em Destination Outpost ARN (ARN do Outpost de destino), insira o ARN do Outpost para o qual deseja copiar o snapshot.
6. (Opcional) Em Description (Descrição), insira uma breve descrição do snapshot copiado.
7. A criptografia é ativada por padrão para a cópia do snapshot. Não é possível desativar a criptografia. Para Chave do KMS, escolha o Chave do KMS a ser usado.
8. Escolha Copiar.

Command line

Para copiar um snapshot de uma região para um Outpost

Use o comando [copy-snapshot](#) (Copiar snapshot). Especifique o ID do snapshot a ser copiado, a região de onde deseja copiar o snapshot e o ARN do Outpost de destino.

Por exemplo, o comando a seguir copia o snapshot snap-1234567890abcdef0 da região us-east-1 para o Outpost arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0.

```
$ aws ec2 copy-snapshot --source-region us-east-1 --source-snapshot-id snap-1234567890abcdef0 --destination-outpost-arn arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0 --description "Local snapshot copy"
```

Copiar AMIs de uma região da AWS para um Outpost

Você pode copiar AMIs de uma região da AWS para um Outpost. Quando você copia uma AMI de uma região para um Outpost, todos os snapshots associados à AMI são copiados da região para o Outpost.

Você pode copiar uma AMI de uma região para uma Outpost somente se os snapshots associados à AMI estiverem na região do Outpost. Se os snapshots estiverem em uma região diferente, você deve copiar primeiro a AMI para a região do Outpost e, em seguida, copiá-lo dessa região para o Outpost.

Note

Você não pode copiar uma AMI de um Outpost para uma região, de um Outpost para outro ou dentro de um Outpost.

Você pode copiar AMIs de uma região para um Outpost usando somente a AWS CLI.

Command line

Para copiar uma AMI de uma região para um Outpost

Use o comando `copy-image` (Copiar imagem). Especifique o ID da AMI a ser copiada, a região de origem e o ARN do Outpost de destino.

Por exemplo, o comando a seguir copia a AMI `ami-1234567890abcdef0` da região `us-east-1` para o Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`.

```
$ aws ec2 copy-image --source-region us-east-1 --source-image-id ami-1234567890abcdef0  
--name "Local AMI copy" --destination-outpost-arn arn:aws:outposts:us-  
east-1:123456789012:outpost/op-1234567890abcdef0
```

Crie volumes a partir de snapshots locais

Você pode criar volumes em Outposts a partir de snapshots locais. Os volumes devem ser criados no mesmo Outpost que os snapshots de origem. Você não pode usar snapshots locais para criar volumes na região para o Outpost.

Ao criar um volume a partir de um snapshot local, você não pode criptografar novamente o volume usando uma Chave do KMS de criptografia diferente. Os volumes criados de snapshots locais devem ser criptografados usando a mesma Chave do KMS que o snapshot de origem.

Para obter mais informações, consulte [Criar um volume a partir de um snapshot \(p. 1270\)](#).

Execute instâncias a partir de AMIs baseadas em snapshots locais

Você pode executar instâncias de AMIs baseadas em snapshots locais. Você deve executar instâncias no mesmo Outpost que a AMI de origem. Para obter mais informações, consulte [Launch an instance on your Outpost](#) (Executar uma instância no Outpost) no Guia do usuário do AWS Outposts.

Exclua snapshots locais

Você pode excluir snapshots locais de um Outpost. Depois de excluir um snapshot de um Outpost, a capacidade de armazenamento do Amazon S3 usada pelo snapshot excluído fica disponível por 72 horas após a exclusão do snapshot e de volumes que fazem referência a esse snapshot.

Como a capacidade de armazenamento do Amazon S3 não fica disponível de forma imediata, recomendamos que você use alarmes Amazon CloudWatch para monitorar a sua capacidade de armazenamento do Amazon S3. Exclua snapshots e volumes de que não precisa mais; assim você previne o fim da capacidade de armazenamento.

Para obter mais informações sobre como excluir snapshots, consulte [Excluir um snapshot \(p. 1316\)](#).

Automatize snapshots em um Outpost

Você pode criar políticas de ciclo de vida do snapshot do Amazon Data Lifecycle Manager que criam, copiam, retêm e excluem snapshots de forma automática de seus volumes e instâncias em um Outpost. Você pode escolher se deseja armazenar os snapshots em uma região ou armazená-los localmente em um Outpost. Além disso, você pode copiar automaticamente snapshots criados e armazenados em uma região da AWS para um Outpost.

A tabela a seguir mostra os fornecimentos e a visão geral de recursos compatíveis.

Localização do recurso	Destino do snapshot	Cópia entre regiões		Restauração rápida de snapshots	Compartilhamento entre contas
		Para a região	Para o Outpost		
Region	Region	✓	✓	✓	✓
Outpost	Region	✓	✓	✓	✓
Outpost	Outpost	✗	✗	✗	✗

Considerations

- No momento, há suporte apenas para as políticas de ciclo de vida de snapshots do Amazon EBS. Não há suporte para políticas de AMI baseadas no EBS e políticas de eventos de compartilhamento entre contas.
- Se uma política gerencia snapshots para volumes ou instâncias em uma região, os snapshots são criados na mesma região que o recurso de origem.
- Se uma política gerencia snapshots para volumes ou instâncias em um Outpost, os snapshots poderão ser criados no Outpost de origem ou na região desse Outpost.
- Uma única política não pode gerenciar snapshots em uma região e snapshots em um Outpost. Se precisar automatizar snapshots em uma região e em um Outpost, você deve criar políticas separadas.
- Não há suporte para a restauração rápida de snapshots para snapshots criados em um Outpost ou copiados para um Outpost.
- Não há suporte para o compartilhamento entre contas para snapshots criados em um Outpost.

Para obter mais informações sobre a criação de um ciclo de vida de snapshot que gerencia snapshots locais, consulte [Automating snapshot lifecycles \(p. 1368\)](#) (Como automatizar ciclos de vida de snapshots).

Usar o APIs diretas do EBS para acessar o conteúdo de um snapshot do EBS

Você pode usar as APIs diretas do Amazon Elastic Block Store (Amazon EBS) para criar snapshots do EBS, gravar dados diretamente nos snapshots, ler dados nos snapshots e identificar as diferenças ou alterações entre dois snapshots. Se você for um provedor independente de software (ISV) que oferece serviços de backup para o Amazon EBS, as APIs diretas do EBS tornarão mais eficiente e econômico rastrear alterações incrementais em seus volumes do EBS por meio de snapshots. Isso pode ser feito sem a necessidade de criar volumes de snapshots e, depois, usar instâncias do Amazon Elastic Compute Cloud (Amazon EC2) para comparar as diferenças.

Você pode criar snapshots incrementais diretamente de dados locais em volumes do EBS e na nuvem a ser usada para recuperação rápida de desastre. Com a capacidade de gravar e ler snapshots, você pode gravar seus dados locais em um snapshot do EBS durante um desastre. Depois, após a recuperação, você pode restaurá-lo de volta para a AWS ou o local a partir do snapshot. Não é mais necessário criar e manter mecanismos complexos para copiar dados de e para o Amazon EBS.

Este guia do usuário fornece uma visão geral dos elementos que compõem as APIs diretas do EBS, e exemplos de como usá-los de maneira eficaz. Para obter mais informações sobre as ações, os tipos de dados, os parâmetros e os erros das APIs, consulte a [referência de APIs diretas do EBS](#). Para obter mais informações sobre as regiões compatíveis da AWS, os endpoints e as cotas de serviço para as APIs diretas do EBS, consulte [Endpoints e cotas do Amazon EBS](#) na Referência geral da AWS.

Tópicos

- [Como entender o APIs diretas do EBS \(p. 1338\)](#)
- [Permissões para usuários do IAM \(p. 1341\)](#)
- [Usar criptografia \(p. 1345\)](#)
- [Usar a assinatura do Signature versão 4. \(p. 1345\)](#)
- [Usar somas de verificação \(p. 1346\)](#)
- [Trabalhar com as APIs diretas do EBS usando a API ou AWS SDKs \(p. 1346\)](#)
- [Como trabalhar com as APIs diretas do EBS usando a linha de comando \(p. 1351\)](#)
- [Otimizar a performance \(p. 1354\)](#)
- [Perguntas frequentes \(p. 1354\)](#)
- [Registrar chamadas de API para as APIs diretas do EBS com o AWS CloudTrail \(p. 1355\)](#)
- [APIs diretas do EBS e VPC endpoints de interface \(p. 1361\)](#)
- [Idempotência para a API StartSnapshot \(p. 1362\)](#)

Como entender o APIs diretas do EBS

Veja a seguir os principais elementos que devem ser compreendidos antes de começar a usar as APIs diretas do EBS.

Pricing

O preço pago por uso das APIs diretas do EBS depende das solicitações feitas. Para obter mais informações, consulte [Definição de preço do Amazon EBS](#).

Snapshots

Os snapshots são o principal meio de fazer backup de dados de volumes do EBS. Com as APIs diretas do EBS, você também pode fazer backup de dados de seus discos locais para snapshots. Para economizar custos de armazenamento, os snapshots sucessivos são incrementais, contendo apenas os dados do volume que mudaram desde o snapshot anterior. Para obter mais informações, consulte [Snapshots do Amazon EBS \(p. 1294\)](#).

Note

Os snapshots públicos não são compatíveis com as APIs diretas do EBS.

Blocks

Um bloco é um fragmento de dados dentro de um snapshot. Cada snapshot pode conter milhares de blocos. Todos os blocos em um snapshot são de tamanho fixo.

Índices de bloco

Um índice de bloco é a posição de deslocamento de um bloco dentro de um snapshot e é usado para identificar o bloco. Multiplique o valor BlockIndex pelo valor BlockSize ($\text{BlockIndex} * \text{BlockSize}$) para identificar o deslocamento lógico dos dados no volume lógico.

Tokens de bloco

Um token de bloco é o hash de identificação de um bloco dentro de um snapshot e é usado para localizar os dados do bloco. Os tokens de bloco retornados pelas APIs diretas do EBS são temporários.

Eles mudam no timestamp de expiração especificado para eles, ou se você executar outra solicitação ListSnapshotBlocks ou ListChangedBlocks para o mesmo snapshot.

Checksum

Uma soma de verificação é um dado de tamanho pequeno derivado de um bloco de dados com a finalidade de detectar erros apresentados durante sua transmissão ou armazenamento. As APIs diretas do EBS usam as somas de verificação para validar a integridade dos dados. Quando você lê dados de um snapshot do EBS, o serviço fornece somas de verificação SHA256 codificadas pelo Base64 para cada bloco de dados transmitidos, que você pode usar para validação. Ao gravar dados em um snapshot do EBS, você deve fornecer uma soma de verificação SHA256 codificada pelo Base64 para cada bloco de dados transmitidos. O serviço valida os dados recebidos usando a soma de verificação fornecida. Para obter mais informações, consulte [Usar somas de verificação \(p. 1346\)](#) adiante neste guia.

Encryption

A criptografia protege seus dados convertendo-os em código ilegível que só pode ser decifrado por pessoas que tiverem acesso à Chave do KMS usada para criptografá-los. Você pode usar as APIs diretas do EBS para ler e gravar snapshots criptografados, mas há algumas limitações. Para obter mais informações, consulte [Usar criptografia \(p. 1345\)](#) adiante neste guia.

Ações da API

As APIs diretas do EBS consistem em seis ações. Há três ações de leitura e três ações de gravação. As ações de leitura são ListSnapshotBlocks, ListChangedBlocks e GetSnapshotBlock. As ações de gravação são StartSnapshot, PutSnapshotBlock e CompleteSnapshot. Essas ações estão descritas nas seções a seguir.

Listar blocos de snapshot

A ação ListSnapshotBlocks retorna os índices e os tokens de bloco dos blocos do snapshot especificado.

Listar blocos alterados

A ação ListChangedBlocks retorna os índices e os tokens de bloco dos blocos que são diferentes entre dois snapshots especificados do mesmo volume e linhagem de snapshots.

Obter bloco de snapshot

A ação GetSnapshotBlock retorna os dados de um bloco para o ID, índice e token de bloco de snapshot especificado.

Iniciar snapshot

A ação StartSnapshot inicia um snapshot, como incremental a partir de um existente ou como um novo snapshot. O snapshot iniciado permanece no estado pendente até ser concluído usando a ação CompleteSnapshot.

Inserir bloco de snapshot

A ação PutSnapshotBlock adiciona dados a um snapshot iniciado na forma de blocos individuais. Especifique uma soma de verificação SHA256 codificada como Base64 para o bloco de dados transmitido. O serviço valida a soma de verificação após a conclusão da transmissão. A solicitação falhará se a soma de verificação calculada pelo serviço não corresponder à que você especificou.

Snapshot completo

A ação CompleteSnapshot conclui um snapshot iniciado que está no estado pendente. Depois, os snapshots são alterados para um estado concluído.

Usar as APIs diretas do EBS para ler snapshots

As etapas a seguir descrevem como usar as APIs diretas do EBS para ler snapshots:

1. Use a ação `ListSnapshotBlocks` para exibir todos os índices e tokens de bloco dos blocos em um snapshot. Ou use a ação `ListChangedBlocks` para exibir apenas os índices e os tokens de bloco dos blocos que são diferentes entre dois snapshots do mesmo volume e linhagem de snapshots. Essas ações ajudam você a identificar os tokens e os índices de bloco dos blocos para os quais você pode querer obter dados.
2. Use a ação `GetSnapshotBlock` e especifique o índice e o token do bloco do qual você deseja obter dados.

Para obter exemplos de como executar essas ações, consulte as seções [Trabalhar com as APIs diretas do EBS usando a API ou AWS SDKs \(p. 1346\)](#) e [Como trabalhar com as APIs diretas do EBS usando a linha de comando \(p. 1351\)](#) mais adiante neste guia.

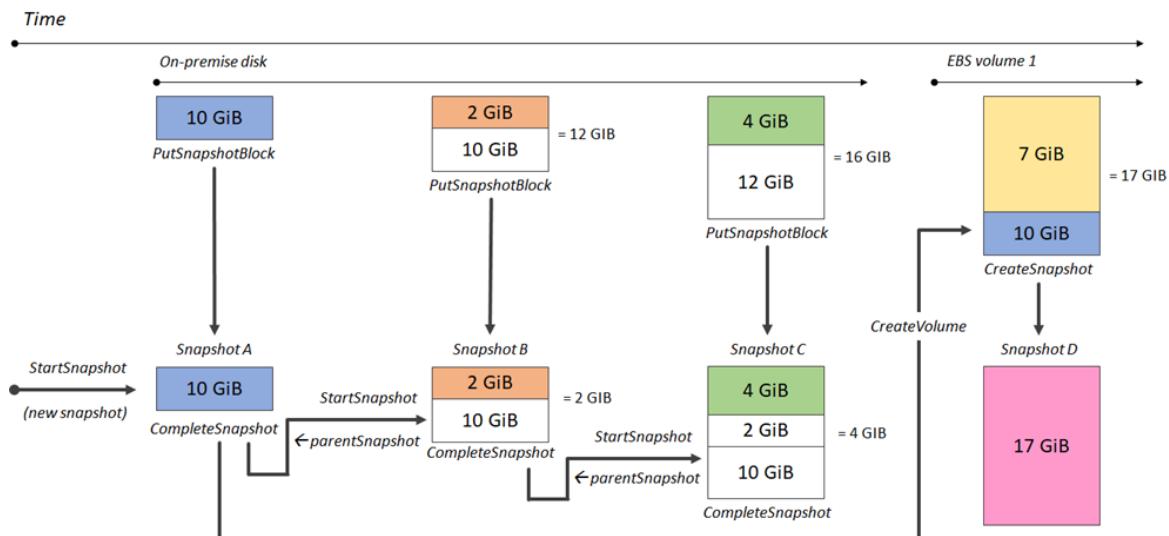
[Usar as APIs diretas do EBS para gravar snapshots incrementais](#)

As etapas a seguir descrevem como usar as APIs diretas do EBS para gravar snapshots incrementais:

1. Use a ação `StartSnapshot` e especifique um ID de snapshot pai para iniciar um snapshot como snapshot incremental de um existente, ou omita o ID do snapshot pai para iniciar um novo snapshot. Essa ação retorna o novo ID de snapshot que está em estado pendente.
2. Use a ação `PutSnapshotBlock` e especifique o ID do snapshot pendente para adicionar dados a ele na forma de blocos individuais. Especifique uma soma de verificação SHA256 codificada como Base64 para o bloco de dados transmitido. O serviço calcula a soma de verificação dos dados recebidos e os valida com relação à soma de verificação especificada. A ação falhará se as somas de verificação não corresponderem.
3. Quando terminar de adicionar dados ao snapshot pendente, use a ação `CompleteSnapshot` para iniciar um fluxo de trabalho assíncrono que sele o snapshot e mova-o para um estado concluído.

Repita essas etapas para criar um novo snapshot incremental usando o snapshot criado anteriormente como pai.

Por exemplo, no diagrama a seguir, o snapshot A é o primeiro novo snapshot iniciado. O snapshot A é usado como snapshot pai para iniciar o snapshot B. O snapshot B é usado como snapshot pai para iniciar e criar o snapshot C. Os snapshots A, B e C são snapshots incrementais. O snapshot A é usado para criar o volume 1 do EBS. O snapshot D é criado a partir do volume 1 do EBS. O snapshot D é um snapshot incremental de A; ele não é um snapshot incremental de B nem C.



Para obter exemplos de como executar essas ações, consulte as seções [Trabalhar com as APIs diretas do EBS usando a API ou AWS SDKs \(p. 1346\)](#) e [Como trabalhar com as APIs diretas do EBS usando a linha de comando \(p. 1351\)](#) mais adiante neste guia.

Permissões para usuários do IAM

Um usuário do AWS Identity and Access Management (IAM) deve ter as políticas a seguir para usar as APIs diretas do EBS. Para obter mais informações, consulte [Alterar permissões para um usuário do IAM](#).

Tenha cuidado ao atribuir as seguintes políticas aos usuários do IAM. Ao atribuir essas políticas, você pode conceder acesso a um usuário que tenha acesso negado ao mesmo recurso por meio das APIs do Amazon EC2, como as ações CopySnapshot ou CreateVolume.

Permissões para ler snapshots

A política a seguir permite que as APIs diretas do EBS de leitura sejam usadas em todos os snapshots em uma região específica da AWS. Na política, substitua `<Region>` pela região do snapshot.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ebs:ListSnapshotBlocks",  
                "ebs:ListChangedBlocks",  
                "ebs:GetSnapshotBlock"  
            ],  
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"  
        }  
    ]  
}
```

A política a seguir permite que a leitura das APIs diretas do EBS seja usada em snapshots com uma tag de chave/valor específica. Na política, substitua `<Key>` pelo valor de chave da tag e `<Value>` pelo valor da tag.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ebs:ListSnapshotBlocks",  
                "ebs:ListChangedBlocks",  
                "ebs:GetSnapshotBlock"  
            ],  
            "Resource": "arn:aws:ec2::snapshot/*",  
            "Condition": {  
                "StringEqualsIgnoreCase": {  
                    "aws:ResourceTag/<Key>": "<Value>"  
                }  
            }  
        }  
    ]  
}
```

A política a seguir permite que todas as APIs diretas do EBS de leitura sejam usadas em todos os snapshots da conta apenas dentro de um intervalo de tempo específico. Essa política autoriza o uso das APIs diretas do EBS com base na chave de condição global `aws:CurrentTime`. Na política, substitua o intervalo de data e hora mostrado pelo intervalo de data e hora da sua política.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ebs>ListSnapshotBlocks",  
                "ebs>ListChangedBlocks",  
                "ebs>GetSnapshotBlock"  
            ],  
            "Resource": "arn:aws:ec2*:snapshot/*",  
            "Condition": {  
                "DateGreaterThan": {  
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"  
                },  
                "DateLessThan": {  
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"  
                }  
            }  
        }  
    ]  
}
```

A política a seguir concede acesso para descriptografar um snapshot criptografado usando uma Chave do KMS específica. Ela concede acesso para criptografar novos snapshots usando o ID de Chave do KMS padrão para snapshots do EBS. Ele também oferece a capacidade de determinar se a criptografia por padrão está habilitada na conta. Na política, substitua `<Region>` pela região da chave do KMS, `<AccountId>` pelo ID da conta da AWS da chave do KMS e `<KeyId>` pelo ID da chave do KMS usada para criptografar o snapshot que você quer ler com as APIs diretas do EBS.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "VisualEditor0",  
            "Effect": "Allow",  
            "Action": [  
                "kms:Encrypt",  
                "kms:Decrypt",  
                "kms:GenerateDataKey",  
                "kms:GenerateDataKeyWithoutPlaintext",  
                "kms:ReEncrypt*",  
                "kms>CreateGrant",  
                "ec2>CreateTags",  
                "kms:DescribeKey",  
                "ec2:GetEbsDefaultKmsKeyId",  
                "ec2:GetEbsEncryptionByDefault"  
            ],  
            "Resource": "arn:aws:kms:<Region>:<AccountId>:key/<KeyId>"  
        }  
    ]  
}
```

Para obter mais informações, consulte [Alteração de permissões para um usuário do IAM](#) no Guia do usuário do IAM.

Permissões para gravar snapshots

A política a seguir permite que as APIs diretas do EBS de gravação sejam usadas em todos os snapshots em uma região específica da AWS. Na política, substitua `<Region>` pela região do snapshot.

```
{
```

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ebs:StartSnapshot",  
                "ebs:PutSnapshotBlock",  
                "ebs:CompleteSnapshot"  
            ],  
            "Resource": "arn:aws:ec2:<Region>::snapshot/*"  
        }  
    ]  
}
```

A política a seguir permite que a gravação das APIs diretas do EBS seja usada em snapshots com uma tag de chave/valor específica. Na política, substitua **<Key>** pelo valor de chave da tag e **<Value>** pelo valor da tag.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ebs:StartSnapshot",  
                "ebs:PutSnapshotBlock",  
                "ebs:CompleteSnapshot"  
            ],  
            "Resource": "arn:aws:ec2:*::snapshot/*",  
            "Condition": {  
                "StringEqualsIgnoreCase": {  
                    "aws:ResourceTag/<Key>": "<Value>"  
                }  
            }  
        }  
    ]  
}
```

A política a seguir permite que todas as APIs diretas do EBS sejam usadas. Ela também permite a ação `StartSnapshot` somente se um ID de snapshot pai for especificado. Portanto, essa política bloqueia a capacidade de iniciar novos snapshots sem o uso de um snapshot pai.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ebs:*",  
            "Resource": "*",  
            "Condition": {  
                "StringEquals": {  
                    "ebs:ParentSnapshot": "arn:aws:ec2:*::snapshot/*"  
                }  
            }  
        }  
    ]  
}
```

A política a seguir permite que todas as APIs diretas do EBS sejam usadas. Ela também permite que apenas a chave de tag `user` seja criada para um novo snapshot. Essa política também garante que o usuário tenha acesso à criação de tags. A ação `StartSnapshot` é a única ação que pode especificar tags.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "ebs:*",  
            "Resource": "*",  
            "Condition": {  
                "ForAllValues:StringEquals": {  
                    "aws:TagKeys": "user"  
                }  
            }  
        },  
        {  
            "Effect": "Allow",  
            "Action": "ec2:CreateTags",  
            "Resource": "*"  
        }  
    ]  
}
```

A política a seguir permite que todas as APIs diretas do EBS de gravação sejam usadas em todos os snapshots da conta apenas dentro de um intervalo de tempo específico. Essa política autoriza o uso das APIs diretas do EBS com base na chave de condição global `aws:CurrentTime`. Na política, substitua o intervalo de data e hora mostrado pelo intervalo de data e hora da sua política.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ebs:StartSnapshot",  
                "ebs:PutSnapshotBlock",  
                "ebs:CompleteSnapshot"  
            ],  
            "Resource": "arn:aws:ec2::snapshot/*",  
            "Condition": {  
                "DateGreaterThan": {  
                    "aws:CurrentTime": "2018-05-29T00:00:00Z"  
                },  
                "DateLessThan": {  
                    "aws:CurrentTime": "2020-05-29T23:59:59Z"  
                }  
            }  
        }  
    ]  
}
```

A política a seguir concede acesso para descriptografar um snapshot criptografado usando uma Chave do KMS específica. Ela concede acesso para criptografar novos snapshots usando o ID de Chave do KMS padrão para snapshots do EBS. Ele também oferece a capacidade de determinar se a criptografia por padrão está habilitada na conta. Na política, substitua `<Region>` pela região da chave do KMS, `<AccountId>` pelo ID da conta da AWS da chave do KMS e `<KeyId>` pelo ID da chave do KMS usada para criptografar o snapshot que você quer ler com as APIs diretas do EBS.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "VisualEditor0",  
            "Effect": "Allow",  
            "Action": "kms:Decrypt",  
            "Resource": "  
                <Region>  
                <AccountId>/AWSKMSDefaultKey/  
                <KeyId>  
            "
```

```
        "Action": [
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:GenerateDataKey",
            "kms:GenerateDataKeyWithoutPlaintext",
            "kms:ReEncrypt*",
            "kms>CreateGrant",
            "ec2:CreateTags",
            "kms:DescribeKey",
            "ec2:GetEbsDefaultKmsKeyId",
            "ec2:GetEbsEncryptionByDefault"
        ],
        "Resource": "arn:aws:kms:<Region>:<AccountId>:key/<KeyId>"
    }
}
```

Para obter mais informações, consulte [Alteração de permissões para um usuário do IAM](#) no Guia do usuário do IAM.

Usar criptografia

Se a criptografia do Amazon EBS por padrão estiver habilitada em sua conta da AWS, você não poderá iniciar um novo snapshot usando um snapshot pai não criptografado. Primeiro, será necessário criptografar o snapshot pai copiando-o. Para obter mais informações, consulte [Copiar um snapshot do Amazon EBS. \(p. 1317\)](#) e [Criptografia por padrão \(p. 1426\)](#).

Para iniciar um snapshot criptografado, especifique o nome de recurso da Amazon (ARN) de uma Chave do KMS ou de um snapshot pai criptografado em sua solicitação StartSnapshot. Se nenhum deles for especificado e a criptografia do Amazon EBS por padrão estiver habilitada na conta, a Chave do KMS padrão da conta será usada. Se nenhuma chave padrão do KMS foi especificada para a conta, a Chave gerenciada pela AWS será usada.

Important

Por padrão, todas as entidades principais da conta têm acesso à Chave gerenciada pela AWS e podem usá-la para operações de criptografia e descriptografia do EBS. Para obter mais informações, consulte [Padrão Chave do KMS para criptografia EBS \(p. 1425\)](#).

Talvez sejam necessárias permissões adicionais do IAM para uso das APIs diretas do EBS com criptografia. Para obter mais informações, consulte a seção [Permissões para usuários do IAM \(p. 1341\)](#) anterior deste guia.

Usar a assinatura do Signature versão 4.

O Signature versão 4 é o processo para adicionar informações de autenticação às solicitações da AWS enviadas por HTTP. Por segurança, a maioria das solicitações para AWS deve ser assinada com uma chave de acesso, que consiste em um ID de chave de acesso e na chave de acesso secreta. Essas duas chaves são comumente conhecidas como suas credenciais de segurança. Para obter informações sobre como obter credenciais para sua conta, consulte [Compreensão e obtenção de suas credenciais](#).

Caso pretenda criar solicitações HTTP manualmente, você deve aprender a assiná-las. Quando você usa a AWS Command Line Interface (AWS CLI) ou um dos AWS SDKs para fazer solicitações à AWS, essas ferramentas assinam automaticamente as solicitações para você com a chave de acesso que você especifica ao configurar as ferramentas. Se você usar essas ferramentas, não precisará saber como assinar solicitações por si mesmo.

Para obter mais informações, consulte [Signing AWS requests with Signature Version 4 \(Assinar solicitações da AWS com o Signature versão 4\)](#) na AWS General Reference (Referência geral da AWS).

Usar somas de verificação

A ação GetSnapshotBlock retorna dados que estão em um bloco de um snapshot, e a ação PutSnapshotBlock adiciona dados a um bloco de um snapshot. Os dados de bloco transmitidos não são assinados como parte do processo de assinatura do Signature versão 4. Como resultado, as somas de verificação são usadas para validar a integridade dos dados da seguinte forma:

- Quando você usa a ação GetSnapshotBlock, a resposta fornece uma soma de verificação SHA256 codificada pelo Base64 para os dados do bloco usando o cabeçalho x-amz-C checksum e o algoritmo de soma de verificação usando o cabeçalho x-amz-C checksum-Algorithm. Use a soma de verificação retornada para validar a integridade dos dados. Se a soma de verificação gerada não corresponder à que o Amazon EBS forneceu, considere os dados não válidos e tente enviar sua solicitação novamente.
- Quando você usa a ação PutSnapshotBlock, sua solicitação deve fornecer uma soma de verificação SHA256 codificada pelo Base64 para os dados do bloco usando o cabeçalho x-amz-C checksum e o algoritmo de soma de verificação usando o cabeçalho x-amz-C checksum-Algorithm. A soma de verificação fornecida é validada com relação a uma soma de verificação gerada pelo Amazon EBS para validar a integridade dos dados. Se as somas de verificação não forem correspondentes, a solicitação falhará.
- Quando você usa a ação CompleteSnapshot, sua solicitação pode, opcionalmente, fornecer uma soma de verificação SHA256 agregada codificada pelo Base64 para o conjunto completo de dados adicionados ao snapshot. Forneça a soma de verificação usando o cabeçalho x-amz-C checksum, o algoritmo de soma de verificação usando o cabeçalho x-amz-C checksum-Algorithm e o método de agregação da soma de verificação usando o cabeçalho x-amz-C checksum-Aggregation-Method. Para gerar a soma de verificação agregada usando o método de agregação linear, organize as somas de verificação para cada bloco gravado na ordem crescente do índice do bloco, concatene-as de modo a formar uma única string e gere a soma de verificação em toda a string usando o algoritmo SHA256.

As somas de verificação nessas ações fazem parte do processo de assinatura do Signature versão 4.

Trabalhar com as APIs diretas do EBS usando a API ou AWS SDKs

A [Referência de APIs diretas do EBS](#) fornece as descrições e a sintaxe de cada uma das ações e dos tipos de dados do serviço. Você também pode usar um dos AWS SDKs para acessar uma API que seja personalizada para a linguagem de programação ou a plataforma que estiver usando. Para obter mais informações, consulte [AWS SDKs](#).

As APIs diretas do EBS exigem uma assinatura do AWS Signature versão 4. Para obter mais informações, consulte [Usar a assinatura do Signature versão 4. \(p. 1345\)](#).

Usar a API para ler snapshots

Listar blocos em um snapshot

A solicitação de exemplo [ListChangedBlocks](#) a seguir retorna os índices e os tokens de bloco dos blocos que estão no snapshot snap-0acEXAMPLEcf41648. O parâmetro startingBlockIndex limita os resultados para índices de bloco maiores que 1000, e o parâmetro maxResults limita os resultados aos primeiros 100 blocos.

```
GET /snapshots/snap-0acEXAMPLEcf41648/blocks?maxResults=100&startingBlockIndex=1000
HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200617T231953Z
Authorization: <Authentication parameter>
```

A resposta de exemplo a seguir para a solicitação anterior lista os índices e os tokens de bloco no snapshot. Use a ação GetSnapshotBlock e especifique o índice e o token do bloco do qual você deseja obter dados. Os tokens de bloco são válidos até o tempo de expiração listado.

```
HTTP/1.1 200 OK
x-amzn-RequestId: d6e5017c-70a8-4539-8830-57f5557f3f27
Content-Type: application/json
Content-Length: 2472
Date: Wed, 17 Jun 2020 23:19:56 GMT
Connection: keep-alive

{
    "BlockSize": 524288,
    "Blocks": [
        {
            "BlockIndex": 0,
            "BlockToken": "AAUBAcuWqOCnDNuKle1ls7IIIX6jp6FYcC/q8oT93913HhvLvA+3JRrSybp/0"
        },
        {
            "BlockIndex": 1536,
            "BlockToken": "AAUBAWudwfmofcrQhGV1LwuRKm2b8ZXPiyrgoykTRC6IU1NbxEWDY1pPjvnV"
        },
        {
            "BlockIndex": 3072,
            "BlockToken": "AAUBAV7p6pC5fKAC7TokoNCtAnZhqq27u6YEXZ3MwRevBkJmMx6iuA6tsBt"
        },
        {
            "BlockIndex": 3073,
            "BlockToken": "AAUBAbqt9zpqBUEvtO2HINAfFaWToOwlPjbIsQ0lx6JUN/0+iMQLONtNbnX4"
        },
        ...
    ],
    "ExpiryTime": 1.59298379649E9,
    "VolumeSize": 3
}
```

Listar blocos diferentes entre dois snapshots

A solicitação de exemplo [ListChangedBlocks](#) a seguir retorna os índices e os tokens de bloco dos blocos que são diferentes entre os snapshots snap-0acEXAMPLEcf41648 e snap-0c9EXAMPLE1b30e2f. O parâmetro startingBlockIndex limita os resultados para índices de bloco maiores que 0, e o parâmetro maxResults limita os resultados aos primeiros 500 blocos.

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/changedblocks?
firstSnapshotId=snap-0acEXAMPLEcf41648&maxResults=500&startingBlockIndex=0 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200617T232546Z
Authorization: <Authentication parameter>
```

A resposta de exemplo a seguir para a solicitação anterior mostra que os índices de bloco 0, 3072, 6002 e 6003 são diferentes entre os dois snapshots. Além disso, os índices de bloco 6002 e 6003 existem somente no primeiro ID de snapshot especificado, e não no segundo ID de snapshot, porque não há um segundo token de bloco listado na resposta.

Use a ação GetSnapshotBlock e especifique o índice e o token do bloco do qual você deseja obter dados. Os tokens de bloco são válidos até o tempo de expiração listado.

```
HTTP/1.1 200 OK
x-amzn-RequestId: fb0f6743-6d81-4be8-afbe-db11a5bb8a1f
```

```
Content-Type: application/json
Content-Length: 1456
Date: Wed, 17 Jun 2020 23:25:47 GMT
Connection: keep-alive

{
    "BlockSize": 524288,
    "ChangedBlocks": [
        {
            "BlockIndex": 0,
            "FirstBlockToken": "AAUBAVaWqOCnDNuKle11s7IIX6jp6FYcC/tJuVT1GgP23AuLntwiMdJ
+OJkL",
            "SecondBlockToken": "AAUBASxzy0Y0b33JVRLoYm3N0resCxn5RO+HVFzXW3Y/
RwfFaPX2Edx8QHCh"
        },
        {
            "BlockIndex": 3072,
            "FirstBlockToken": "AAUBAcHp6pC5fKAC7TokoNCtAnZhqq27u6fxRfZOLEmeXLmHBf2R/
Yb24MaS",
            "SecondBlockToken": "AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid"
        },
        {
            "BlockIndex": 6002,
            "FirstBlockToken": "AAABASqX4/
NWjvNceoyMULjcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
        },
        {
            "BlockIndex": 6003,
            "FirstBlockToken": "AAABASmJ005JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKof4PBROuICb2A"
        },
        ...
    ],
    "ExpiryTime": 1.592976647009E9,
    "VolumeSize": 3
}
```

Obter dados de bloco de um snapshot

O exemplo [GetSnapshotBlock](#) a seguir retorna os dados no índice de bloco 3072 com o token de bloco AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid, no snapshot snap-0c9EXAMPLE1b30e2f.

```
GET /snapshots/snap-0c9EXAMPLE1b30e2f/blocks/3072?
blockToken=AAUBARGCaufCqBRZC8tEkPYGGkSv3vqvOjJ2xKDi3ljDFiytUxBLXYgTmkid HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200617T232838Z
Authorization: <Authentication parameter>
```

A resposta de exemplo a seguir para a solicitação anterior mostra o tamanho dos dados retornados, a soma de verificação para validar os dados e o algoritmo usado para gerar a soma de verificação. Os dados binários são transmitidos no corpo da resposta e representados como [BlockData](#) no exemplo a seguir.

```
HTTP/1.1 200 OK
x-amzn-RequestId: 2d0db2fb-bd88-474d-a137-81c4e57d7b9f
x-amz-Data-Length: 524288
x-amz-C checksum: Vc0yY2j3gg8bUL9I6GQuI2orTudrQRBDMIhc7bdEsw=
x-amz-C checksum-Algorithm: SHA256
Content-Type: application/octet-stream
```

```
Content-Length: 524288
Date: Wed, 17 Jun 2020 23:28:38 GMT
Connection: keep-alive
```

BlockData

Usar a API para gravar snapshots incrementais

Iniciar um snapshot

A solicitação de exemplo [StartSnapshot](#) a seguir inicia um snapshot 8 GiB usando o snapshot `snap-123EXAMPLE1234567` como snapshot pai. O novo snapshot será um snapshot incremental do snapshot pai. O snapshot será movido para um estado de erro se não houver solicitações `put` ou `complete` feitas para o snapshot dentro do período limite especificado de 60 minutos. O token `550e8400-e29b-41d4-a716-446655440000` do cliente garante idempotência para a solicitação. Se o token do cliente for omitido, o SDK da AWS gerará um automaticamente. Para obter mais informações sobre idempotência, consulte [Idempotência para a API StartSnapshot \(p. 1362\)](#).

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": "snap-123EXAMPLE1234567",
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

O exemplo de resposta a seguir para a solicitação anterior mostra o ID do snapshot, o ID da conta da AWS, o status, o tamanho do volume em GiB e o tamanho dos blocos no snapshot. O snapshot é iniciado em estado pendente. Especifique o ID do snapshot em uma solicitação `PutSnapshotBlocks` subsequente para gravar dados no snapshot.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 929e6eb9-7183-405a-9502-5b7da37c1b18
Content-Type: application/json
Content-Length: 181
Date: Thu, 18 Jun 2020 04:07:29 GMT
Connection: keep-alive

{
    "BlockSize": 524288,
    "Description": null,
    "OwnerId": "138695307491",
    "Progress": null,
    "SnapshotId": "snap-052EXAMPLEc85d8dd",
    "StartTime": null,
    "Status": "pending",
    "Tags": null,
    "VolumeSize": 8
}
```

Inserir dados em um snapshot

A solicitação de exemplo [PutSnapshot](#) a seguir grava 524288 bytes de dados no índice de bloco 1000 no snapshot `snap-052EXAMPLEc85d8dd`. A soma de verificação

QOD3gmEQQXATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM= codificada pelo Base64 foi gerada com o uso do algoritmo SHA256. Os dados são transmitidos no corpo da solicitação e representados como **BlockData** no exemplo a seguir.

```
PUT /snapshots/snap-052EXAMPLEc85d8dd/blocks/1000 HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-Data-Length: 524288
x-amz-C checksum: QOD3gmEQQXATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM=
x-amz-C checksum-Algorithm: SHA256
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T042215Z
X-Amz-Content-SHA256: UNSIGNED-PAYLOAD
Authorization: <Authentication parameter>
```

BlockData

Veja a seguir a resposta de exemplo para a solicitação anterior, que confirma o comprimento dos dados, a soma de verificação e o algoritmo de soma de verificação para os dados recebidos pelo serviço.

```
HTTP/1.1 201 Created
x-amzn-RequestId: 643ac797-7e0c-4ad0-8417-97b77b43c57b
x-amz-C checksum: QOD3gmEQQXATfJx2Aa34W4FU2nZGyXfqtsUukt0w8DM=
x-amz-C checksum-Algorithm: SHA256
Content-Type: application/json
Content-Length: 2
Date: Thu, 18 Jun 2020 04:22:12 GMT
Connection: keep-alive

{}
```

Concluir um snapshot

A solicitação de exemplo [CompleteSnapshot](#) a seguir conclui o snapshot **snap-052EXAMPLEc85d8dd**. O comando especifica que 5 blocos foram gravados no snapshot. A soma de verificação **6D3nmwi5f2F0wlh7xX8QprrrJBFzDX8aacdOcA3KCM3c=** representa a soma de verificação para o conjunto completo de dados gravados em um snapshot.

```
POST /snapshots/completion/snap-052EXAMPLEc85d8dd HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
x-amz-ChangedBlocksCount: 5
x-amz-C checksum: 6D3nmwi5f2F0wlh7xX8QprrrJBFzDX8aacdOcA3KCM3c=
x-amz-C checksum-Algorithm: SHA256
x-amz-C checksum-Aggregation-Method: LINEAR
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T043158Z
Authorization: <Authentication parameter>
```

Veja a seguir um exemplo de resposta para a solicitação anterior.

```
HTTP/1.1 202 Accepted
x-amzn-RequestId: 06cba5b5-b731-49de-af40-80333ac3a117
Content-Type: application/json
Content-Length: 20
Date: Thu, 18 Jun 2020 04:31:50 GMT
Connection: keep-alive

{"Status": "pending"}
```

Como trabalhar com as APIs diretas do EBS usando a linha de comando

Os exemplos a seguir mostram como usar APIs diretas do EBS usando a AWS Command Line Interface (AWS CLI). Para obter mais informações sobre como instalar e configurar a AWS CLI, consulte [Instalar a AWS CLI](#) e [Configuração rápida da AWS CLI](#).

Usar as AWS CLI para ler snapshots

Listar blocos em um snapshot

O comando de exemplo `list-snapshot-blocks` a seguir retorna os índices e os tokens de bloco dos blocos que estão no snapshot `snap-0987654321`. O parâmetro `--starting-block-index` limita os resultados para índices de bloco maiores que 1000, e o parâmetro `--max-results` limita os resultados aos primeiros 100 blocos.

```
aws ebs list-snapshot-blocks --snapshot-id snap-0987654321 --starting-block-index 1000 --  
max-results 100
```

A resposta de exemplo a seguir para o comando anterior lista os índices e os tokens de bloco no snapshot. Use o comando `get-snapshot-block` e especifique o índice e o token do bloco do qual você deseja obter dados. Os tokens de bloco são válidos até o tempo de expiração listado.

```
{  
    "Blocks": [  
        {  
            "BlockIndex": 1001,  
            "BlockToken": "AAABAV3/PNhXOynVdMYHUpPsetaSvjLB1dtIGfbJv5OJ0sX855EzGTWos4a4"  
        },  
        {  
            "BlockIndex": 1002,  
            "BlockToken": "AAABATGQIgwr0WwIuqIMjCA/Sy7e/YoQFZsHejzGNvjKauzNgzeI13YHBfQB"  
        },  
        {  
            "BlockIndex": 1007,  
            "BlockToken": "AAABAZ9CTuQtUvp/dxqRWw4d07e0gTZ3jvn6hiW30W9duM8MiMw6yQayzF2c"  
        },  
        {  
            "BlockIndex": 1012,  
            "BlockToken": "AAABAQdzxhw0rVV6PNmsfo/YRIxo9JPR85XxPf1BLjg0Hec6pygYr6laE1p0"  
        },  
        {  
            "BlockIndex": 1030,  
            "BlockToken": "AAABAAaYvPax6mv+iGWLdTUjQtFWouQ7Dqz6nSD9L+CbXnvpkswA6iIDID523d"  
        },  
        {  
            "BlockIndex": 1031,  
            "BlockToken": "AAABATgWZC0XcFwUKvTJbUXMiSPg59KVxJGL+BWBC1kw6spzCxJVqDVaTskJ"  
        },  
        ...  
    ],  
    "ExpiryTime": 1576287332.806,  
    "VolumeSize": 32212254720,  
    "BlockSize": 524288  
}
```

Listar blocos diferentes entre dois snapshots

O comando de exemplo `list-changed-blocks` a seguir retorna os índices e os tokens de bloco dos blocos que são diferentes entre os snapshots `snap-1234567890` e `snap-0987654321`. O parâmetro `--starting-block-index` limita os resultados para índices de bloco maiores que 0, e o parâmetro `--max-results` limita os resultados aos primeiros 500 blocos.

```
aws ebs list-changed-blocks --first-snapshot-id snap-1234567890 --second-snapshot-id snap-0987654321 --starting-block-index 0 --max-results 500
```

A resposta de exemplo a seguir para o comando anterior mostra que os índices de bloco 0, 6000, 6001, 6002 e 6003 são diferentes entre os dois snapshots. Além disso, os índices de bloco 6001, 6002 e 6003 existem somente no primeiro ID de snapshot especificado, e não no segundo ID de snapshot, porque não há um segundo token de bloco listado na resposta.

Use o comando `get-snapshot-block` e especifique o índice e o token do bloco do qual você deseja obter dados. Os tokens de bloco são válidos até o tempo de expiração listado.

```
{
    "ChangedBlocks": [
        {
            "BlockIndex": 0,
            "FirstBlockToken": "AAABAVahm9SO60Dyi0ORySzn2ZjGjW/KN3uygG1s0QOYWesbzBbDnX2dGpmC",
            "SecondBlockToken":
                "AAABAf8o0o6UFi1rDbSZGIRaCEdDyBu9TlvtCQxxoKV8qrUPQP7vcM6iWGsr"
        },
        {
            "BlockIndex": 6000,
            "FirstBlockToken": "AAABAbYSiZvJ0/R9tz8suI8dSzecLjN4kkazK8inFXVintPkdaVFLfCMQsKe",
            "SecondBlockToken":
                "AAABAZnqTdzFmKRpsaMAsDxviVqEI/3jJzI2crq2eFDCgHmyNf777elD9oVR"
        },
        {
            "BlockIndex": 6001,
            "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jb5Q6FRXFqAIAqE04hJoR"
        },
        {
            "BlockIndex": 6002,
            "FirstBlockToken": "AAABASqX4/NWjvNceoyMULjcRd0DnwbSwNnes1UkoP62CrQXvn47BY5435aw"
        },
        {
            "BlockIndex": 6003,
            "FirstBlockToken":
                "AAABASmJ005JxAOce25rF4P1sdRtyIDsX12tFEDunnePYUKOf4PBROuICb2A"
        },
        ...
    ],
    "ExpiryTime": 1576308931.973,
    "VolumeSize": 32212254720,
    "BlockSize": 524288,
    "NextToken": "AAADARqElNng/sV98CYk/bJDCXeLJmLJHnNSkHvLzVaO0zsPH/QM3Bi3zF//O6Mdi/BbJarBnp8h"
}
```

Obter dados de bloco de um snapshot

O comando de exemplo `get-snapshot-block` a seguir retorna os dados no índice de bloco 6001 com o token de bloco `AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jb5Q6FRXFqAIAqE04hJoR`, no snapshot `snap-1234567890`. Os dados binários serão enviados para o arquivo `data` no diretório `C:\Temp` em um computador Windows. Se você executar o comando em um computador Linux ou Unix, substitua o caminho de saída por `/tmp/data` para enviar os dados ao arquivo `data` no diretório `/tmp`.

```
aws ebs get-snapshot-block --snapshot-id snap-1234567890 --block-index 6001 --block-token AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jb5Q6FRXFqAIAqE04hJoR C:/Temp/data
```

A resposta de exemplo a seguir para o comando anterior mostra o tamanho dos dados retornados, a soma de verificação para validar os dados e o algoritmo da soma de verificação. Os dados binários são salvos automaticamente no diretório e no arquivo especificados no comando da solicitação.

```
{  
    "DataLength": "524288",  
    "Checksum": "cf0Y6/FnOoFa4VyjQPOa/iD0zhTf1PTKzxGv2OKowXc=",  
    "ChecksumAlgorithm": "SHA256"  
}
```

Usar as AWS CLI para gravar snapshots incrementais

Iniciar um snapshot

O comando de exemplo [start-snapshot](#) a seguir inicia um snapshot 8 GiB usando o snapshot snap-123EXAMPLE1234567 como snapshot pai. O novo snapshot será um snapshot incremental do snapshot pai. O snapshot será movido para um estado de erro se não houver solicitações put ou complete feitas para o snapshot dentro do período limite especificado de 60 minutos. O token 550e8400-e29b-41d4-a716-446655440000 do cliente garante idempotência para a solicitação. Se o token do cliente for omitido, o SDK da AWS gerará um automaticamente. Para obter mais informações sobre idempotência, consulte [Idempotência para a API StartSnapshot \(p. 1362\)](#).

```
aws ebs start-snapshot --volume-size 8 --parent-snapshot snap-123EXAMPLE1234567 --  
timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

O exemplo de resposta a seguir para o comando anterior mostra o ID do snapshot, o ID da conta da AWS, o status, o tamanho do volume em GiB e o tamanho dos blocos no snapshot. O snapshot é iniciado em estado pending. Especifique o ID do snapshot nos comandos [put-snapshot-block](#) subsequentes para gravar dados no snapshot, depois, use o comando [complete-snapshot](#) para concluir o snapshot e alterar seu status para completed.

```
{  
    "SnapshotId": "snap-0aaEXAMPLEe306d62",  
    "OwnerId": "111122223333",  
    "Status": "pending",  
    "VolumeSize": 8,  
    "BlockSize": 524288  
}
```

Inserir dados em um snapshot

O comando de exemplo [put-snapshot](#) a seguir grava 524288 bytes de dados no índice de bloco 1000 no snapshot snap-0aaEXAMPLEe306d62. A soma de verificação QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= codificada pelo Base64 foi gerada com o uso do algoritmo SHA256. Os dados transmitidos ficam no arquivo /tmp/data.

```
aws ebs put-snapshot-block --snapshot-id snap-0aaEXAMPLEe306d62  
--block-index 1000 --data-length 524288 --block-data /tmp/data --  
checksum QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM= --checksum-algorithm SHA256
```

A resposta de exemplo a seguir para o comando anterior confirma o comprimento dos dados, a soma de verificação e o algoritmo de soma de verificação para os dados recebidos pelo serviço.

```
{  
    "DataLength": "524288",  
    "Checksum": "QOD3gmEQOXATfJx2Aa34W4FU2nZGyXfqtsUuktOw8DM=",  
    "ChecksumAlgorithm": "SHA256"
```

}

Concluir um snapshot

O comando de exemplo `complete-snapshot` a seguir conclui o snapshot `snap-0aaEXAMPLEe306d62`. O comando especifica que 5 blocos foram gravados no snapshot. A soma de verificação `6D3nmwi5f2F0wlh7xX8QprJBFzDX8aacdOcA3KCM3c=` representa a soma de verificação para o conjunto completo de dados gravados em um snapshot. Para obter mais informações sobre somas de verificação, consulte [Usar somas de verificação \(p. 1346\)](#) anteriormente neste guia.

```
aws ebs complete-snapshot --snapshot-id snap-0aaEXAMPLEe306d62 --changed-blocks-count 5  
--checksum 6D3nmwi5f2F0wlh7xX8QprJBFzDX8aacdOcA3KCM3c= --checksum-algorithm SHA256 --  
checksum-aggregation-method LINEAR
```

Veja a seguir um exemplo de resposta para o comando anterior.

```
{  
    "Status": "pending"  
}
```

Otimizar a performance

Você pode executar solicitações de API simultaneamente. Supondo que a latência PutSnapshotBlock seja de 100ms, um thread poderá processar 10 solicitações em um segundo. Além disso, supondo que a aplicação do cliente crie vários threads e conexões (por exemplo, 100 conexões), ela poderá fazer 1000 ($10 * 100$) solicitações por segundo no total. Isso corresponde a uma taxa de transferência de cerca de 500 MB por segundo.

A lista a seguir contém alguns itens a serem observados na aplicação:

- Cada thread está usando uma conexão distinta? Se as conexões são limitadas na aplicação, vários threads aguardarão a disponibilidade da conexão e você perceberá uma taxa de transferência menor.
- Há algum tempo de espera na aplicação entre duas solicitações put? Isso reduzirá a taxa de transferência efetiva de um thread.
- O limite de largura de banda na instância: se a largura de banda na instância for compartilhada por outras aplicações, ela poderá limitar a taxa de transferência disponível para solicitações PutSnapshotBlock.

Para evitar gargalos, certifique-se de observar outras workloads que podem estar em execução na conta. Você também deve criar mecanismos de repetição nos fluxos de trabalho de APIs diretas do EBS para lidar com o controle de utilização, os tempos limite e a indisponibilidade do serviço.

Revise as cotas de serviço das APIs diretas do EBS para determinar o número máximo de solicitações de API que você pode executar por segundo. Para obter mais informações, consulte [Amazon Elastic Block Store endpoints and quotas](#) (Endpoints e cotas do Amazon Elastic Block Store) na AWS General Reference (Referência geral da AWS).

Perguntas frequentes

Um snapshot pode ser acessado usando as APIs diretas do EBS se tiver um status pendente?

Não. O snapshot só poderá ser acessado se tiver um status concluído.

Os índices de bloco são retornados pelas APIs diretas do EBS em ordem numérica?

Sim. Os índices de bloco retornados são exclusivos e em ordem numérica.

Posso enviar uma solicitação com um valor de parâmetro MaxResults inferior a 100?

Não. O valor mínimo permitido do parâmetro MaxResults é 100. Se você enviar uma solicitação com um valor de parâmetro MaxResult inferior a 100 e houver mais de 100 blocos no snapshot, a API retornará pelo menos 100 resultados.

Posso executar solicitações de API simultaneamente?

Você pode executar solicitações de API simultaneamente. Para evitar gargalos, certifique-se de observar outras workloads que podem estar em execução na conta. Você também deve criar mecanismos de repetição nos fluxos de trabalho de APIs diretas do EBS para lidar com o controle de utilização, os tempos limite e a indisponibilidade do serviço. Para obter mais informações, consulte [Otimizar a performance \(p. 1354\)](#).

Revise as cotas de serviço das APIs diretas do EBS para determinar o número de solicitações de API que você pode executar por segundo. Para obter mais informações, consulte [Amazon Elastic Block Store endpoints and quotas](#) (Endpoints e cotas do Amazon Elastic Block Store) na AWS General Reference (Referência geral da AWS).

Ao executar a ação ListChangedBlocks, é possível obter uma resposta vazia mesmo que haja blocos no snapshot?

Sim. Se os blocos alterados forem escassos no snapshot, a resposta poderá ser vazia, mas a API retornará um valor de token de próxima página. Use o valor de token de próxima página para continuar na próxima página de resultados. Você pode confirmar que atingiu a última página de resultados quando a API retornar um valor nulo de token de próxima página.

Se o parâmetro NextToken for especificado junto com um parâmetro StartingBlockIndex, qual dos dois será usado?

O NextToken será usado e o StartingBlockIndex será ignorado.

Por quanto tempo os tokens de bloco e os próximos tokens são válidos?

Os tokens de bloco são válidos por sete dias e os próximos tokens são válidos por 60 minutos.

Há suporte para snapshots criptografados?

Sim. Os snapshots criptografados podem ser acessados usando as APIs diretas do EBS.

Para acessar um snapshot criptografado, o usuário deve ter acesso à chave do KMS usada para criptografar o snapshot e à ação de descriptografia do AWS KMS. Consulte a seção [Permissões para usuários do IAM \(p. 1341\)](#) anterior deste guia para obter a política do AWS KMS a ser atribuída a um usuário.

Há suporte para snapshots públicos?

Snapshots públicos não são compatíveis.

A listagem de blocos do snapshot retorna todos os índices e os tokens de bloco em um snapshot, ou somente aqueles que têm dados gravados neles?

Ela retorna somente os índices e os tokens de bloco que têm dados gravados neles.

Posso obter um histórico das chamadas de API realizadas pelas APIs diretas do EBS na minha conta para fins de análise de segurança ou solução de problemas operacionais?

Sim. Para receber um histórico de chamadas de API de APIs diretas do EBS feitas em sua conta, ative o AWS CloudTrail no AWS Management Console. Para obter mais informações, consulte [Registrar chamadas de API para as APIs diretas do EBS com o AWS CloudTrail \(p. 1355\)](#).

[Registrar chamadas de API para as APIs diretas do EBS com o AWS CloudTrail](#)

O serviço de APIs diretas do EBS é integrado ao AWS CloudTrail. O AWS CloudTrail é um serviço que fornece um registro de ações, executadas por um usuário, uma função ou um produto da AWS. O

CloudTrail captura todas as chamadas de API realizadas nas APIs diretas do EBS como eventos. Ao criar uma trilha, você poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon Simple Storage Service (Amazon S3). Se você não configurar uma trilha, ainda poderá visualizar os eventos de gerenciamento mais recentes no console do CloudTrail em Event history (Histórico de eventos). Os eventos de dados não são capturados no histórico de eventos. Você pode usar as informações coletadas pelo CloudTrail para determinar a solicitação feita a APIs diretas do EBS, o endereço IP da solicitação, quem fez a solicitação, quando ela foi feita e outros detalhes.

Para obter mais informações sobre o CloudTrail, consulte o [Manual do usuário do AWS CloudTrail](#).

Informações de APIs diretas do EBS no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade de evento compatível em APIs diretas do EBS, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de produtos da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e fazer download de eventos recentes em sua conta da AWS. Para obter mais informações, consulte [Como visualizar eventos com o histórico de eventos do CloudTrail](#).

Para ter um registro contínuo de eventos em sua conta da AWS, incluindo os eventos de APIs diretas do EBS, crie uma trilha. Uma trilha permite que o CloudTrail forneça arquivos de log para um bucket do S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e fornece os arquivos de log ao bucket do S3 que você especificar. Além disso, você pode configurar outros produtos da AWS para analisar mais profundamente e agir sobre os dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)
- [Serviços e integrações compatíveis com o CloudTrail](#)
- [Configuração de notificações do Amazon SNS para o CloudTrail](#)
- [Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas](#)

Ações de API compatíveis

Para APIs diretas do EBS, é possível usar o CloudTrail para registrar dois tipos de eventos:

- Eventos de gerenciamento: eventos de gerenciamento fornecem visibilidade em operações de gerenciamento que são executadas nos snapshots de sua conta da AWS. Por padrão, as seguintes ações de API são registradas como eventos de gerenciamento em trilhas:
 - [StartSnapshot](#)
 - [CompleteSnapshot](#)

Para obter mais informações sobre como registrar eventos de gerenciamento, consulte [Registrar eventos de gerenciamento para trilhas](#) no Manual do usuário do CloudTrail.

- Eventos de dados: estes eventos fornecem visibilidade nas operações do snapshot executadas no snapshot ou dentro de um snapshot. Opcionalmente, as seguintes ações de API podem ser registradas como eventos de dados em trilhas:
 - [ListSnapshotBlocks](#)
 - [ListChangedBlocks](#)
 - [GetSnapshotBlock](#)
 - [PutSnapshotBlock](#)

Eventos de dados não são registrados por padrão quando você cria uma trilha. É possível usar apenas seletores de eventos avançados para registrar eventos de dados em chamadas diretas de API do EBS. Para obter mais informações, consulte [Registrar eventos de dados para trilhas](#) no Manual do usuário do CloudTrail.

Note

Ao executar uma ação em um snapshot compartilhado com você, os eventos de dados não serão enviados à conta da AWS do proprietário do snapshot.

Informações de identidade

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte [userIdentityElement do CloudTrail](#).

Compreender as entradas do arquivo de log de APIs diretas do EBS

Uma trilha é uma configuração que permite a entrega de eventos como registros de log a um bucket do S3 especificado. Os arquivos de log do CloudTrail contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer origem e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

A seguir, estão exemplos de entradas de log do CloudTrail.

StartSnapshot

```
{  
    "eventVersion": "1.05",  
    "userIdentity": {  
        "type": "IAMUser",  
        "principalId": "123456789012",  
        "arn": "arn:aws:iam::123456789012:root",  
        "accountId": "123456789012",  
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
        "userName": "user"  
    },  
    "eventTime": "2020-07-03T23:27:26Z",  
    "eventSource": "ebs.amazonaws.com",  
    "eventName": "StartSnapshot",  
    "awsRegion": "eu-west-1",  
    "sourceIPAddress": "192.0.2.0",  
    "userAgent": "PostmanRuntime/7.25.0",  
    "requestParameters": {  
        "volumeSize": 8,  
        "clientToken": "token",  
        "encrypted": true  
    },  
    "responseElements": {  
        "snapshotId": "snap-123456789012",  
        "ownerId": "123456789012",  
        "status": "pending",  
        "startTime": "Jul 3, 2020 11:27:26 PM",  
        "volumeSize": 8,  
        "blockSize": 524288,  
        "volumeType": "standard"  
    }  
}
```

```
        "kmsKeyArn": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

CompleteSnapshot

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2020-07-03T23:28:24Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "CompleteSnapshot",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "PostmanRuntime/7.25.0",
    "requestParameters": {
        "snapshotId": "snap-123456789012",
        "changedBlocksCount": 5
    },
    "responseElements": {
        "status": "completed"
    },
    "requestID": "be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
    "eventID": "6e12345-2a4e-417c-aa78-7594fEXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

ListSnapshotBlocks

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-03T00:32:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListSnapshotBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example6-0e12-4aa9-b923-1555eexample",
}
```

```
"eventID": "example4-218b-4f69-a9e0-2357dexample",
"readOnly": true,
"resources": [
    {
        "accountId": "123456789012",
        "type": "AWS::EC2::Snapshot",
        "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
    }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "123456789012",
"eventCategory": "Data",
"tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-SHA",
    "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
}
}
```

ListChangedBlocks

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:11:46Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "ListChangedBlocks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "firstSnapshotId": "snap-abcdef01234567890",
        "secondSnapshotId": "snap-9876543210abcdef0",
        "maxResults": 100,
        "startingBlockIndex": 0
    },
    "responseElements": null,
    "requestID": "example0-f4cb-4d64-8d84-72e1bexample",
    "eventID": "example3-fac4-4a78-8ebb-3e9d3example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-abcdef01234567890"
        },
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2::snapshot/snap-9876543210abcdef0"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
```

```
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

GetSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T20:43:05Z",
    "eventSource": "ebs.amazonaws.com",
    "eventName": "GetSnapshotBlock",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "111.111.111.111",
    "userAgent": "PostmanRuntime/7.28.0",
    "requestParameters": {
        "snapshotId": "snap-abcdef01234567890",
        "blockIndex": 1,
        "blockToken": "EXAMPLEil5E3pMPFpaDWjExM2/mnSKh1mQfcbjwe2mM7EwhrgCdPAEXAMPLE"
    },
    "responseElements": null,
    "requestID": "examplea-6eca-4964-abfd-fd9f0example",
    "eventID": "example6-4048-4365-a275-42e94example",
    "readOnly": true,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::EC2::Snapshot",
            "ARN": "arn:aws:ec2:us-west-2:snapshot/snap-abcdef01234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "123456789012",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-SHA",
        "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
    }
}
```

PutSnapshotBlock

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAT4HPB2AO3JEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/user",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "user"
    },
    "eventTime": "2021-06-02T21:09:17Z",
```

```
"eventSource": "ebs.amazonaws.com",
"eventName": "PutSnapshotBlock",
"awsRegion": "us-east-1",
"sourceIPAddress": "111.111.111.111",
"userAgent": "PostmanRuntime/7.28.0",
"requestParameters": {
    "snapshotId": "snap-abcdef01234567890",
    "blockIndex": 1,
    "dataLength": 524288,
    "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
    "checksumAlgorithm": "SHA256"
},
"responseElements": {
    "checksum": "exampleodSGvFSb1e3kxWUgbOQ4TbzPurnsfVexample",
    "checksumAlgorithm": "SHA256"
},
"requestID": "example3-d5e0-4167-8ee8-50845example",
"eventID": "example8-4d9a-4aad-b71d-bb31fexample",
"readOnly": false,
"resources": [
    {
        "accountId": "123456789012",
        "type": "AWS::EC2::Snapshot",
        "ARN": "arn:aws:ec2:us-west-2:snapshot/snap-abcdef01234567890"
    }
],
"eventType": "AwsApiCall",
"managementEvent": false,
"recipientAccountId": "123456789012",
"eventCategory": "Data",
"tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-SHA",
    "clientProvidedHostHeader": "ebs.us-west-2.amazonaws.com"
}
}
```

APIs diretas do EBS e VPC endpoints de interface

É possível estabelecer uma conexão privada entre a VPC e as APIs diretas do EBS criando um endpoint da VPC de interface. Os endpoints de interface são habilitados por [AWS PrivateLink](#), uma tecnologia que permite acessar de forma privada as APIs diretas do EBS sem um gateway da Internet, um dispositivo NAT, uma conexão VPN ou uma conexão do AWS Direct Connect. As instâncias na VPC não precisam de endereços IP públicos para a comunicação com APIs diretas do EBS. O tráfego de rede entre a VPC e as APIs diretas do EBS não deixa a rede da Amazon.

Cada endpoint de interface é representado por uma ou mais [interfaces de rede elástica](#) nas sub-redes.

Para obter mais informações, consulte [VPC endpoints de interface \(AWS PrivateLink\)](#) no Guia do usuário da Amazon VPC.

Considerações para endpoints da VPC de APIs diretas do EBS

Antes de configurar um endpoint da VPC de interface para endpoints de APIs diretas do EBS do Amazon RDS, revise [Interface endpoint properties and limitations](#) (Propriedades e limitações do endpoint de interface) no Amazon VPC User Guide (Manual do usuário da Amazon VPC).

As políticas de endpoint da VPC não são compatíveis com APIs diretas do EBS. Por padrão, o acesso total às APIs diretas do EBS é permitido pelo endpoint. No entanto, é possível controlar o acesso ao endpoint de interface usando grupos de segurança. Para obter mais informações, consulte [Controlar o acesso a serviços com VPC endpoints](#) no Guia do usuário da Amazon VPC.

Criar um endpoint da VPC de interface para APIs diretas do EBS

É possível criar um endpoint da VPC para APIs diretas do EBS usando o console da Amazon VPC ou a AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte [Criar um endpoint de interface](#) no Manual do usuário da Amazon VPC.

Criar um endpoint da VPC para APIs diretas do EBS usando o seguinte nome de serviço:

- com.amazonaws.*region*.ebs

Se você habilitar o DNS privado para o endpoint, poderá fazer solicitações de API para as APIs diretas do EBS usando seu nome DNS padrão para a região, por exemplo, ebs.us-east-1.amazonaws.com. Para obter mais informações, consulte [Acessar um serviço por um endpoint de interface](#) no Guia do usuário da Amazon VPC.

Idempotência para a API StartSnapshot

A idempotência garante que uma solicitação de API seja concluída apenas uma vez. Com uma solicitação idempotente, se a solicitação original for concluída com êxito, as novas tentativas subsequentes retornam o resultado da solicitação original bem-sucedida e não terão efeito adicional.

A API [StartSnapshot](#) oferece suporte para idempotência usando um token do cliente. Um token de cliente é uma string exclusiva que você especifica ao fazer uma solicitação de API. Se você tentar refazer uma solicitação de API com o mesmo token de cliente e os mesmos parâmetros de solicitação depois de ela ter sido concluída com êxito, o resultado da solicitação original será retornado. Se você tentar refazer uma solicitação com o mesmo token de cliente, mas alterar um ou mais parâmetros de solicitação, o erro `ConflictException` será retornado.

Se você não especificar seu próprio token de cliente, os SDKs da AWS gerarão automaticamente um token de cliente para a solicitação a fim de garantir idempotência.

Um token de cliente pode ser qualquer string que inclua até 64 caracteres ASCII. Não reutilize os mesmos tokens de cliente para solicitações diferentes.

Como fazer uma solicitação StartSnapshot idempotente com seu próprio token de cliente usando a API Especifique o parâmetro de solicitação `ClientToken`.

```
POST /snapshots HTTP/1.1
Host: ebs.us-east-2.amazonaws.com
Accept-Encoding: identity
User-Agent: <User agent parameter>
X-Amz-Date: 20200618T040724Z
Authorization: <Authentication parameter>

{
    "VolumeSize": 8,
    "ParentSnapshot": snap-123EXAMPLE1234567,
    "ClientToken": "550e8400-e29b-41d4-a716-446655440000",
    "Timeout": 60
}
```

Como fazer uma solicitação StartSnapshot idempotente com seu próprio token de cliente usando a AWS CLI

Especifique o parâmetro de solicitação `client-token`.

```
C:\> aws ebs start-snapshot --region us-east-2 --volume-size 8 --parent-snapshot
snap-123EXAMPLE1234567 --timeout 60 --client-token 550e8400-e29b-41d4-a716-446655440000
```

Automatizar o ciclo de vida do snapshot

Você pode usar o Amazon Data Lifecycle Manager para automatizar a criação, retenção e exclusão de snapshots usados para fazer backup de seus volumes do Amazon EBS.

Para obter mais informações, consulte [Amazon Data Lifecycle Manager \(p. 1363\)](#).

Amazon Data Lifecycle Manager

Você pode usar o Amazon Data Lifecycle Manager para automatizar a criação, a retenção e a exclusão de snapshots do EBS e de AMIs apoiadas pelo EBS. Quando você automatiza o gerenciamento de snapshot e AMI, isso ajuda a:

- Proteger dados valiosos impondo uma programação regular de backup.
- Crie AMIs padronizadas que podem ser atualizadas em intervalos regulares.
- Reter os backups conforme exigido por auditores ou pelas regras de conformidade interna.
- Reduzir os custos de armazenamento ao excluir backup obsoletos.
- Criar políticas de backup de recuperação de desastres que fazem backup de dados em contas isoladas.

Quando combinado com os recursos de monitoramento do Amazon CloudWatch Events e do AWS CloudTrail, o Amazon Data Lifecycle Manager oferece uma solução completa de backup para instâncias de Amazon EC2 e volumes do EBS sem custo adicional.

Important

O Amazon Data Lifecycle Manager não pode ser usado para gerenciar snapshots ou AMIs criados por qualquer outro meio.

O Amazon Data Lifecycle Manager não pode ser usado para automatizar a criação, retenção e exclusão de AMIs com armazenamento de instâncias.

Tópicos

- [Como Amazon Data Lifecycle Manager funciona \(p. 1363\)](#)
- [Considerações para o Amazon Data Lifecycle Manager \(p. 1366\)](#)
- [Automação dos ciclos de vida do snapshot \(p. 1368\)](#)
- [Automatizar ciclos de vida da AMI \(p. 1376\)](#)
- [Automatizar cópias de snapshots entre contas \(p. 1382\)](#)
- [Exibir, modificar e excluir políticas de ciclo de vida \(p. 1390\)](#)
- [AWS Identity and Access Management \(p. 1394\)](#)
- [Monitorar o ciclo de vida de snapshots e AMIs \(p. 1400\)](#)

Como Amazon Data Lifecycle Manager funciona

Veja a seguir os elementos de chaves do Amazon Data Lifecycle Manager.

Elementos

- [Snapshots \(p. 1364\)](#)
- [AMIs apoiadas pelo EBS \(p. 1364\)](#)
- [Tags de recurso de destino \(p. 1364\)](#)
- [Tags do Amazon Data Lifecycle Manager \(p. 1364\)](#)
- [Políticas de ciclo de vida \(p. 1364\)](#)

- [Programações de política \(p. 1365\)](#)

Snapshots

Os snapshots são o principal meio de fazer backup de dados de volumes do EBS. Para economizar custos de armazenamento, os snapshots sucessivos são incrementais, contendo apenas os dados do volume que mudaram desde o snapshot anterior. Quando você exclui um snapshot de uma série de snapshots de um volume, somente os dados exclusivos daquele snapshot são removidos. Os dados restantes do histórico capturado do volume são preservados.

Para obter mais informações, consulte [Snapshots do Amazon EBS \(p. 1294\)](#).

AMIs apoiadas pelo EBS

Uma Imagem de máquina da Amazon (AMI) fornece as informações necessárias para iniciar uma instância. Você pode executar várias instâncias em uma única AMI quando precisa de várias instâncias com a mesma configuração. O Amazon Data Lifecycle Manager é compatível apenas com AMIs com EBS. AMIs apoiadas pelo EBS incluem um snapshot para cada volume do EBS associado à instância de origem.

Para obter mais informações, consulte [Imagens de máquina da Amazon \(AMIs\) \(p. 22\)](#).

Tags de recurso de destino

O Amazon Data Lifecycle Manager usa tags de recursos para identificar os recursos para fazer backup. As tags são metadados personalizáveis que você pode atribuir aos recursos da AWS (inclusive instâncias do Amazon EC2, volumes do EBS e snapshots). Uma política do Amazon Data Lifecycle Manager (descrita posteriormente) segmenta uma instância ou um volume para backup usando uma única tag. Várias tags podem ser atribuídas a uma instância ou volume se você quiser executar várias políticas neles.

Não é possível usar o caractere “\” ou “=” em uma chave de tag.

Para obter mais informações, consulte [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#).

Tags do Amazon Data Lifecycle Manager

O Amazon Data Lifecycle Manager aplica as seguintes tags a todos os snapshots e AMIs criados por uma política a fim de distingui-los dos snapshots e AMIs criados por outros meios:

- `aws:dlm:lifecycle-policy-id`
- `aws:dlm:lifecycle-schedule-name`
- `aws:dlm:expirationTime`
- `dlm:managed`

Você também pode especificar tags personalizadas para aplicar durante a criação de um snapshot e AMIs. Não é possível usar o caractere “\” ou “=” em uma chave de tag.

As tags de destino que o Amazon Data Lifecycle Manager usa para associar os volumes à política podem ser aplicadas opcionalmente aos snapshots criados pela política. Da mesma forma, as tags de destino usadas para associar instâncias a uma política de AMI podem, opcionalmente, ser aplicadas às AMIs criadas pela política.

Políticas de ciclo de vida

Uma política de ciclo de vida consiste nessas configurações principais:

- **Tipo de política:** define o tipo de recursos que a política pode gerenciar. O Amazon Data Lifecycle Manager é compatível com os seguintes tipos de políticas de ciclo de vida:

- Política de ciclo de vida de snapshot—Usada para automatizar o ciclo de vida dos snapshots do EBS. Essas políticas podem se destinar a volumes individuais do EBS ou a todos os volumes do EBS anexados a uma instância.
- Política de ciclo de vida da AMI baseada no EBS: usada para automatizar o ciclo de vida das AMIs baseadas no EBS e os snapshots de base. Essas políticas só podem direcionar instâncias.
- Política de eventos de cópia entre contas: usada para automatizar cópias de snapshots entre contas. Use essa política em conjunto com uma política de snapshot do EBS que compartilha snapshots entre contas.
- Tipo de recurso—Define tipos de recursos que são direcionados pela política. As políticas de ciclo de vida do snapshot podem direcionar instâncias ou volumes. Use VOLUME para criar snapshots de volumes individuais ou use INSTANCE para criar snapshots de vários volumes de todos os volumes associados a uma instância. Para obter mais informações, consulte [Snapshots de vários volumes \(p. 1299\)](#). As políticas de ciclo de vida da AMI só podem direcionar instâncias. Uma AMI é criada que inclui snapshots de todos os volumes associados à instância de destino.
- Tags de destino—Especifica as tags que devem ser associadas a um volume do EBS ou a uma instância do Amazon EC2 a ser gerenciada pela política.
- Programações—As horas de início e os intervalos para a criação de snapshots ou AMIs. A primeira operação de criação de snapshot ou AMI começa uma hora após o horário de início especificado. As operações de criação de snapshot ou AMI subsequentes começam uma hora após o horário programado. Uma política pode ter até quatro programações – uma programação obrigatória e até três programações opcionais. Para obter mais informações, consulte [Programações de política \(p. 1365\)](#).
- Retenção—Especifica como os snapshots ou AMIs devem ser retidos. Você pode reter snapshots ou AMIs com base na contagem total (baseada em contagem) ou na idade (baseada na idade). Para políticas de snapshot, quando o limite de retenção é atingido, o snapshot mais antigo é excluído. Para políticas de AMI, quando o limite de retenção é atingido, a AMI mais antiga é cancelada e seus snapshots de backup são excluídos.

Por exemplo, você pode criar uma política com configurações semelhantes às seguintes:

- Gerencia todos os volumes do EBS que têm uma tag com uma chave de account e um valor de finance.
- Cria snapshots a cada 24 horas em 0900 UTC.
- Mantém apenas os cinco snapshots mais recentes.
- Inicia a criação de snapshot o mais tardar em 0959 UTC a cada dia.

Programações de política

As programações de política definem quando os snapshots ou AMIS são criados pela política. As políticas podem ter até quatro programações — uma obrigatória e até três opcionais.

Adicionar várias programações a uma única política permite que você crie snapshots ou AMIs em frequências diferentes usando a mesma política. Por exemplo, você pode criar uma única política que cria snapshots diários, semanais, mensais e anuais. Isso elimina a necessidade de gerenciar várias políticas.

Para cada programação, você pode definir a frequência, configurações de restauração rápida de snapshot (somente políticas de ciclo de vida do snapshot), regras de cópia entre regiões e tags. As etiquetas atribuídas a um agendamento são automaticamente atribuídas aos snapshots ou AMIs criados quando o agendamento é iniciado. Além disso, o Amazon Data Lifecycle Manager atribui automaticamente uma tag gerada pelo sistema com base na frequência da programação a cada snapshot ou AMI.

Cada agendamento é acionado individualmente com base na frequência. Se vários agendamentos forem iniciados ao mesmo tempo, o Amazon Data Lifecycle Manager criará apenas um snapshot ou uma AMI e aplicará as configurações de retenção do agendamento que tem o período de retenção mais alto. As etiquetas de todos os agendamentos iniciados são aplicadas ao snapshot ou à AMI.

- (Somente políticas de ciclo de vida de snapshot) Se mais de um dos agendamentos iniciados estiver habilitado para restauração rápida de snapshots, o snapshot será habilitado para restauração rápida de snapshots em todas as zonas de disponibilidade especificadas em todos os agendamentos iniciados. As configurações de retenção mais altas dos agendamentos iniciados são usadas para cada zona de disponibilidade.
- Se mais de um dos agendamentos iniciados estiver habilitado para cópia entre regiões, o snapshot ou a AMI serão copiados para todas as regiões especificadas em todos os agendamentos iniciados. O período de retenção mais alta dos agendamentos iniciados é aplicado.

Considerações para o Amazon Data Lifecycle Manager

A conta da AWS tem as seguintes cotas relacionadas ao Amazon Data Lifecycle Manager.

- Você pode criar até 100 políticas de ciclo de vida por região.
- Você pode adicionar até 45 tags por recurso.

As seguintes considerações se aplicam a políticas de ciclo de vida:

- Uma política não começa a criar snapshots até você definir o status de ativação como habilitado. Você pode configurar uma política de forma que ela fique habilitada no momento da criação.
- A primeira operação de criação de snapshot ou AMI começa uma hora após o horário de início especificado. As operações de criação de snapshot ou AMI subsequentes começam uma hora após o horário programado.
- Se você modificar uma política removendo ou alterando suas tags de destino, os volumes do EBS que possuem essas tags não serão mais afetados pela política.
- Se você alterar o nome da programação de uma política, os snapshots criados sob o antigo nome da programação não serão mais afetados pela política.
- Se você modificar uma programação de retenção baseada em tempo para usar um novo intervalo de tempo, o novo intervalo será usado somente para novos snapshots ou AMIs criados após a alteração. A nova programação não afeta a programação de retenção de snapshots ou AMIs criados antes da alteração.
- Não é possível alterar a programação de retenção de uma política de acordo com a contagem para baseada no tempo após a criação. Para fazer essa alteração, você deve criar uma nova política.
- Se você desabilitar uma política com uma programação de retenção baseada em idade, os snapshots ou AMIs definidos para expirar enquanto a política estiver desativada serão mantidos indefinidamente. Você deve excluir os snapshots ou cancelar o registro das AMIs manualmente. Quando você habilitar a política novamente, o Amazon Data Lifecycle Manager retoma a exclusão de snapshots à medida que seus períodos de retenção expiram.
- Se você excluir o recurso com retenção baseada em contagem ao qual a política se aplica, ela não poderá mais gerenciar os snapshots ou AMIs previamente criados. Você deve excluir manualmente os snapshots ou cancelar o registro das AMIs se eles não forem mais necessários.
- Se você excluir o recurso ao qual se aplica uma política com retenção baseada na idade, a política continuará a excluir snapshots ou a cancelar o registro de AMIs na programação definida, até, mas sem incluir, o último snapshot ou AMI. Você deve excluir manualmente o último snapshot ou cancelar o registro da última AMI, se ele não for mais necessário.
- Você pode criar várias políticas para fazer backup de um volume do EBS ou uma instância do Amazon EC2. Por exemplo, se um volume do EBS tem duas tags, onde a tag A é um destino da política A para criar um snapshot a cada 12 horas, e a tag B é um destino da política B para criar um snapshot a cada 24 horas, o Amazon Data Lifecycle Manager cria snapshots de acordo com as programações de ambas as políticas. Como alternativa, você pode obter o mesmo resultado criando uma única política que tenha várias programações. Por exemplo, você pode criar uma única política que segmenta apenas a tag A, e especificar duas programações—uma para cada 12 horas e uma para cada 24 horas.

- Se você criar uma política que segmenta instâncias e novos volumes forem associados à instância após a criação da política, os volumes recém-adicionados serão incluídos no backup na próxima execução da política. Todos os volumes associados à instância no momento da execução da política são incluídos.
- Para políticas de ciclo de vida da AMI, quando o limite de retenção da AMI é atingido, a AMI mais antiga é cancelada e seus snapshots de backup são excluídos.
- Se uma política com um cronograma personalizado baseado em cron e uma regra de retenção baseada em idade ou baseada em contagem estiver configurada para criar apenas um snapshot ou uma AMI, a política não excluirá automaticamente este snapshot ou AMI quando o limite de retenção for atingido. Você deve excluir manualmente o snapshot ou cancelar o registro da AMI, se ele não for mais necessário.

As seguintes considerações se aplicam às políticas de ciclo de vida e à [restauração rápida de snapshots \(p. 1434\)](#):

- Um snapshot habilitado para restauração rápida continua habilitado mesmo que você exclua ou desabilite a política de ciclo de vida ou desabilite a restauração rápida de snapshots para a zona de disponibilidade. É possível desabilitar a restauração rápida desses snapshots manualmente.
- Se você habilitar a recuperação rápida de snapshots e exceder o número máximo de snapshots que podem ser habilitados para restauração rápida de snapshots, o Amazon Data Lifecycle Manager criará snapshots, mas não os habilitará para restauração rápida. Depois que um snapshot que está habilitado para restauração rápida for excluído, o próximo snapshot que o Amazon Data Lifecycle Manager criar será habilitado para restauração rápida.
- Quando você habilita a restauração rápida de um snapshot, são necessários 60 minutos por TiB para otimizar o snapshot. Recomendamos criar uma programação que garanta que cada snapshot seja totalmente otimizado antes que o Amazon Data Lifecycle Manager crie o próximo snapshot.
- Você será cobrado por cada minuto em que a restauração rápida de snapshots estiver habilitada para um snapshot em uma determinada zona de disponibilidade. As cobranças são divididas com um mínimo de uma hora. Para obter mais informações, consulte [Definição de preço e cobrança \(p. 1438\)](#).

Note

Dependendo da configuração de suas políticas de ciclo de vida, você pode ter vários snapshots habilitados para restauração rápida de snapshots simultaneamente.

As considerações a seguir se aplicam ao compartilhamento de snapshots entre contas:

- Você só pode compartilhar snapshots não criptografados ou criptografados usando uma chave gerenciada pelo cliente gerenciada pelo cliente.
- Você não pode compartilhar snapshots criptografados com a Chave do KMS de criptografia padrão do EBS.
- Se você compartilhar snapshots criptografados, também deverá compartilhar a Chave do KMS usada para criptografar o volume de origem com as contas de destino. Para obter mais informações, consulte [Allowing users in other accounts to use a KMS key](#) (Permitir que usuários de outras contas usem uma CMK) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

As seguintes considerações se aplicam às políticas de eventos de cópia entre contas:

- Você só pode copiar snapshots não criptografados ou criptografados usando uma chave gerenciada pelo cliente.
- Você pode criar uma política de eventos de cópia entre contas que copia snapshots compartilhados fora do Amazon Data Lifecycle Manager.
- Se você quiser criptografar snapshots na conta de destino, a função do IAM selecionada para a política de eventos de cópia entre contas deve ter permissão para usar a Chave do KMS necessária.

As considerações a seguir se aplicam às políticas de AMI baseadas no EBS e à defasagem de AMI:

- Se você aumentar a contagem de defasagem da AMI para uma programação com retenção baseada em contagem, a alteração será aplicada a todas as AMIs (atuais e novas) criadas pela programação.
- Se você aumentar o período de defasagem da AMI para uma programação com retenção baseada em idade, a alteração será aplicada somente a novas AMIs. AMIs atuais não são afetadas.
- Se você remover a regra de defasagem da AMI de uma programação, o Amazon Data Lifecycle Manager não cancelará a defasagem de AMIs que foram anteriormente consideradas defasadas por essa programação.
- Se você diminuir a contagem ou período de defasagem da AMI de uma programação, o Amazon Data Lifecycle Manager não cancelará a defasagem de AMIs que foram anteriormente consideradas defasadas por essa programação.
- Se você defasar manualmente uma AMI criada por uma política de AMI, o Amazon Data Lifecycle Manager não substituirá a defasagem.
- Se você cancelar manualmente a defasagem de uma AMI que foi anteriormente defasada por uma política de AMI, o Amazon Data Lifecycle Manager não substituirá o cancelamento.
- Se uma AMI for criada por várias programações conflitantes e uma ou mais dessas programações não tiverem uma regra de defasagem da AMI, o Amazon Data Lifecycle Manager não vai defasar essa AMI.
- Se uma AMI for criada por várias programações conflitantes e todas essas programações tiverem uma regra de defasagem da AMI, o Amazon Data Lifecycle Manager não vai defasar essa AMI.

Automação dos ciclos de vida do snapshot

O procedimento a seguir mostra como usar o Amazon Data Lifecycle Manager para automatizar os ciclos de vida de snapshots do Amazon EBS.

Use um dos procedimentos a seguir para criar uma política de ciclo de vida de snapshots.

New console

Para criar uma política de snapshot

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Na tela Select policy type (Selecionar tipo de política), escolha EBS snapshot policy (Política de snapshot do EBS) e depois Next (Próximo).
4. Na seção Target resources (Recursos de destino), faça o seguinte:
 - a. Em Target resource types, (Tipos de recurso de destino), escolha o tipo de recurso para backup. Escolha Volume (Volume) para criar snapshots de volumes individuais ou Instance (Instância) para criar snapshots multivolume dos volumes associados a uma instância.
 - b. (Somente para clientes avançados do AWS Outpost) Em Target resource location (Localização do recurso de destino), especifique onde os recursos de origem estão localizados.
 - Se os recursos de origem estiverem localizados em uma região da AWS, escolha AWS Region (Região da AWS). O Amazon Data Lifecycle Manager faz backup de todos os recursos do tipo especificado que têm etiquetas de destino correspondentes somente na região atual. Se o recurso estiver localizado em uma região, os snapshots criados pela política serão armazenados na mesma região.
 - Se os recursos de origem estiverem localizados em um Outpost em sua conta, escolha AWS Outpost. O Amazon Data Lifecycle Manager faz backup de todos os recursos do

tipo especificado que tenham etiquetas de destino correspondentes em todos os Outposts em sua conta. Se o recurso estiver localizado em um Outpost, os snapshots criados pela política poderão ser armazenados na mesma região ou no mesmo Outpost que o recurso.

- Caso não tenha o Outposts em sua conta, essa opção será oculta e a região da AWS será selecionada para você.
- c. Em Target with these tags (Destino com essas etiquetas), escolha as etiquetas de recurso que identificam os volumes ou as instâncias dos quais fazer backup. A política só oferece suporte aos recursos com a chave de tag e os pares de valor especificados.
 5. Para Description (Descrição), insira uma breve descrição da rota.
 6. Em IAM role (Função do IAM), selecione a função do IAM que tem permissões para gerenciar snapshots e para descrever volumes e instâncias. Para usar a função padrão fornecida pelo Amazon Data Lifecycle Manager, escolha Default role (Função padrão). Se preferir, para usar uma função do IAM personalizada criada anteriormente, selecione Choose another role (Escolher outra função) e selecione a função a ser usada.
 7. Em Policy tags (Etiquetas de políticas), adicione as etiquetas a serem aplicadas na política de ciclo de vida. Você pode usar essas etiquetas para identificar e categorizar suas políticas.
 8. Em Policy status after creation (Status da política após a criação), selecione Enable policy (Habilitar política) para iniciar as execuções da política no próximo horário agendado ou Disable policy (Desabilitar política) para impedir que a política seja executada. Se você não habilitar a política agora, ela não começará a criar snapshots até que você a ative manualmente após a criação.
 9. Escolha Next (Próximo).
 10. Em Configure schedule (Configurar agendamento), configure os agendamentos de política. Uma política pode ter até quatro agendamentos. A Programação 1 é obrigatória. As Programações 2, 3 e 4 são opcionais. Para cada agendamento de política que você adicionar, faça o seguinte:
 - a. Na seção Schedule details (Detalhes do agendamento), faça o seguinte:
 - i. Em Schedule name (Nome do agendamento), especifique um nome descritivo para o agendamento.
 - ii. Em Frequency (Frequência) e nos campos relacionados, configure o intervalo entre as execuções da política. É possível configurar execuções de políticas com uma programação diária, semanal, mensal ou anual. Como opção, escolha Custom cron expression (Expressão cron personalizada) para especificar um intervalo de até 1 ano. Para obter mais informações, consulte [Cron expressions](#) (Expressões cron) no Guia do usuário do Amazon CloudWatch Events.
 - iii. Em Starting at (Iniciando às), especifique a hora em que as execuções da política estão programadas para iniciar. A primeira execução da política começa uma hora depois do horário agendado. A hora deve ser inserida no formato hh:mm UTC.
 - iv. Em Retention type (Tipo de retenção), especifique a política de retenção para snapshots criados pelo agendamento. Você pode reter snapshots com base na contagem total ou na idade deles.

Para retenção baseada em contagem, o intervalo é de 1 a 1000. Quando a contagem máxima for atingida, o snapshot mais antigo será excluído quando um novo for criado.

Para retenção baseada na idade, o intervalo é de 1 dia a 100 anos. Depois que o período de retenção de cada snapshot expirar, ele será excluído.

Note

Todas as programações devem ter o mesmo tipo de retenção. Você pode especificar o tipo de retenção somente para a Programação 1. As Programações 2, 3 e 4 herdam o tipo de retenção da Programação 1. Cada programação pode ter sua própria contagem ou período de retenção.

- v. (Somente para clientes do AWS Outposts) Em Snapshot destination (Destino do snapshot), especifique o destino dos snapshots criados pela política.
 - Se a política se destina aos recursos de uma região, os snapshots devem ser criados na mesma região da AWS A região está selecionada para você.
 - Se a política se destina aos recursos de um Outpost, é possível escolher criar os snapshots no mesmo Outpost que o recurso de origem ou na região que está associada ao Outpost.
 - Caso não tenha o Outposts em sua conta, essa opção será oculta, e a região da AWS será selecionada para você.
- b. Na seção Tagging (Marcação), faça o seguinte:
 - i. Para copiar todas as etiquetas definidas por usuário do volume de origem para os snapshots criados pelo agendamento, selecione Copy tags from source (Copiar etiquetas da origem).
 - ii. Para especificar etiquetas adicionais a serem atribuídas aos snapshots criados por esse agendamento, escolha Add tags (Adicionar etiquetas).
- c. Para habilitar a restauração rápida de snapshots para snapshots criados pelo agendamento, na seção Fast snapshot restore (Restauração rápida de snapshots), selecione Enable fast snapshot restore (Habilitar restauração rápida de snapshots). Se você habilitar a restauração rápida de snapshots, deverá escolher as zonas de disponibilidade nas quais serão habilitadas. Se o agendamento usar uma programação de retenção baseada em idade, será necessário especificar o período para o qual habilitar a restauração rápida de snapshots para cada snapshot. Se o agendamento usar retenção baseada em contagem, será necessário especificar o número máximo de snapshots para ativar a restauração rápida de snapshots.

Se o agendamento criar snapshots em um Outpost, você não poderá habilitar a restauração rápida de snapshots. A restauração rápida de snapshots não é compatível com snapshots locais armazenados em um Outpost.

Note

Você será cobrado por cada minuto em que a restauração rápida de snapshots estiver habilitada para um snapshot em uma determinada zona de disponibilidade. As cobranças são divididas com um mínimo de uma hora.

- d. Para copiar snapshots criados pelo agendamento para um Outpost ou para uma região diferente, na seção Cross-Region copy (Cópia entre regiões), selecione Enable cross-Region copy (Habilitar cópia entre regiões).

Se a política criar snapshots em uma região, você poderá copiar os snapshots para até três regiões ou Outposts adicionais em sua conta. Você deve especificar uma regra de cópia entre regiões separada para cada região ou Outpost de destino.

Para cada região ou Outpost, você pode escolher diferentes políticas de retenção e se deseja copiar todas as tags ou nenhuma. Se o snapshot de origem estiver criptografado, ou se a criptografia estiver habilitada por padrão, os snapshots copiados serão criptografados. Se o snapshot de origem não estiver criptografado, você poderá habilitar a criptografia. Se você não especificar uma chave do KMS, os snapshots serão criptografados usando a chave do KMS padrão de criptografia do EBS em cada região de destino. Se você especificar uma Chave do KMS para a região de destino, a função do IAM selecionada deverá ter acesso à Chave do KMS.

Note

É necessário garantir que o número de cópias de snapshots simultâneas não seja excedido por região.

Se a política criar snapshots em um Outpost, você não poderá copiá-los para uma região ou outro Outpost e as configurações de cópia entre regiões não estarão disponíveis.

- e. Em Cross-account sharing (Compartilhamento entre contas), configure a política para compartilhar automaticamente os snapshots criados pelo agendamento com outras contas da AWS. Faça o seguinte:
 - i. Para habilitar o compartilhamento com outras contas da AWS, selecione Enable cross-account sharing (Habilitar o compartilhamento entre contas).
 - ii. Para adicionar contas com as quais os snapshots serão compartilhados, escolha Add account (Adicionar conta), insira o ID de 12 dígitos da conta da AWS e escolha Add (Adicionar).
 - iii. Para cancelar o compartilhamento de snapshots compartilhados automaticamente após um período específico, selecione Unshare automatically (Cancelar o compartilhamento automaticamente). Se você escolher cancelar automaticamente o compartilhamento de snapshots compartilhados, o período após o qual cancelar o compartilhamento automaticamente dos snapshots não poderá ser maior do que o período para o qual a política retém seus snapshots. Por exemplo, se a configuração de retenção da política retém snapshots por um período de cinco dias, você pode configurar a política para cancelar o compartilhamento automático de snapshots compartilhados após períodos de até quatro dias. Isso se aplica a políticas com configurações de retenção de snapshots baseadas em idade e em contagem.
 - f. Para adicionar outros agendamentos, escolha Add another schedule (Adicionar outro agendamento), localizado na parte superior da tela. Para cada agendamento adicional, preencha os campos conforme descrito anteriormente neste tópico.
 - g. Depois de adicionar os agendamentos necessários, escolha Review policy (Revisar política).
11. Revise o resumo da política e escolha Create policy (Criar política).

Old console

Para criar uma política de snapshot

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Forneça as seguintes informações para sua política, conforme necessário:
 - Description (Descrição)—Uma descrição da política.
 - Policy type (Tipo de política)—O tipo de política a ser criada. Selecione EBS snapshot policy (Política de snapshots do EBS).
 - Resource type (Tipo de recurso): o tipo do recurso para backup. Escolha Volume (Volume) para criar snapshots de volumes individuais ou Instance (Instância) para criar snapshots multivolume dos volumes associados a uma instância.
 - Resource location (Local do recurso): local dos recursos para backup. Se os recursos de origem estiverem localizados em uma região da AWS, escolha AWS Region (Região da AWS). Se os recursos de origem estiverem localizados em um Outpost em sua conta, escolha AWS Outpost. Se você escolher o AWS Outpost, o Amazon Data Lifecycle Manager fará o backup de

todos os recursos do tipo especificado que tenham etiquetas de destino correspondentes em todos os Outposts de sua conta.

Se você não tiver Outposts em sua conta, a AWS Region (Região da AWS) será selecionada por padrão.

Note

Se o recurso estiver localizado em uma região, os snapshots criados pela política serão armazenados na mesma região. Se o recurso estiver localizado em um Outpost, os snapshots criados pela política poderão ser armazenados na mesma região ou no mesmo Outpost que o recurso.

- Target with these tags ((Destino com estas tags)) — as tags de recursos que identificam os volumes ou as instâncias dos quais fazer backup. A política só oferece suporte aos recursos com a chave de tag e os pares de valor especificados.
 - Lifecycle policy (Política de ciclo de vida): as etiquetas a serem aplicadas à política de ciclo de vida.
4. Em IAM role (função do IAM), escolha a função do IAM que tiver permissões para criar, excluir e descrever snapshots e para descrever volumes e instâncias. A AWS fornece uma função padrão, ou você pode criar uma função do IAM personalizada.
 5. Adicione as programações de política. A Programação 1 é obrigatória. As Programações 2, 3 e 4 são opcionais. Para cada programação de política que você incluir, especifique as seguintes informações:
 - Schedule name—(Nome da programação): um nome para a programação.
 - Frequency (Frequência)—: o intervalo entre as execuções da política. É possível configurar execuções de políticas com uma programação diária, semanal, mensal ou anual. Como opção, escolha Custom cron expression (Expressão cron personalizada) para especificar um intervalo de até 1 ano. Para obter mais informações, consulte [Cron expressions](#) (Expressões cron) no Guia do usuário do Amazon CloudWatch Events.
 - Iniciar às hh:mm UTC—a hora em que as execuções da política estão programadas para iniciar. A primeira execução da política começa uma hora depois do horário agendado.
 - Retention type (Tipo de retenção): é possível reter snapshots com base na contagem total ou na idade. Para retenção baseada em contagem, o intervalo é de 1 a 1000. Quando a contagem máxima for atingida, o snapshot mais antigo será excluído quando um novo for criado. Para retenção baseada na idade, o intervalo é de 1 dia a 100 anos. Depois que o período de retenção de cada snapshot expirar, ele será excluído. O período de retenção deve ser maior ou igual ao intervalo.

Note

Todas as programações devem ter o mesmo tipo de retenção. Você pode especificar o tipo de retenção somente para a Programação 1. As Programações 2, 3 e 4 herdam o tipo de retenção da Programação 1. Cada programação pode ter sua própria contagem ou período de retenção.

- Snapshot destination (Destino do snapshot): especifica o destino dos snapshots criados pela política. Para criar snapshots na mesma região da AWS que o recurso de origem, escolha AWSRegion (Região da AWS). Para criar snapshots em um Outpost, escolhaAWS Outpost.

Se a política atinge os recursos em uma região, os snapshots serão criados na mesma região e não poderão ser criados em um Outpost.

Se a política atinge os recursos em um Outpost, os snapshots poderão ser criados no mesmo Outpost que o recurso de origem ou na região associada ao Outpost.

- Copy tags from source (Copiar etiquetas da origem): escolha se deseja copiar todas as etiquetas definidas pelo usuário do volume de origem para os snapshots ou as AMIs criadas pelo agendamento.
- Variable tags (Etiquetas variáveis): se o recurso de origem for uma instância, você pode optar por etiquetar automaticamente seus snapshots com as seguintes etiquetas de variáveis:
 - `instance-id`—O ID da instância de origem.
 - `timestamp`: a data e a hora da execução da política.
- Additional tags (Etiquetas adicionais): especifique quaisquer etiquetas adicionais a serem atribuídas aos snapshots criados por esse agendamento.
- Fast snapshot restore (Restauração rápida de snapshots): escolha se deseja ativar a restauração rápida de snapshots para todos os snapshots criados pelo agendamento. Se você habilitar a restauração rápida de snapshots, deverá escolher as zonas de disponibilidade nas quais serão habilitadas. Você será cobrado por cada minuto em que a restauração rápida de snapshots estiver habilitada para um snapshot em uma determinada zona de disponibilidade. As cobranças são divididas com um mínimo de uma hora. Também é possível especificar o número máximo de snapshots que podem ser habilitados para restauração rápida de snapshots.

Se a política criar snapshots em um Outpost, você não poderá habilitar a restauração rápida de snapshots. A restauração rápida de snapshots não é compatível com snapshots locais armazenados em um Outpost.

- Cross region copy (Cópia entre regiões): se a política criar snapshots em uma região, você poderá copiar os snapshots para até três regiões ou Outposts adicionais em sua conta. Você deve especificar uma regra de cópia entre regiões separada para cada região ou Outpost de destino.

Para cada região ou Outpost, você pode escolher diferentes políticas de retenção e se deseja copiar todas as tags ou nenhuma. Se o snapshot de origem estiver criptografado, ou se a criptografia estiver habilitada por padrão, os snapshots copiados serão criptografados. Se o snapshot de origem não estiver criptografado, você poderá habilitar a criptografia. Se você não especificar uma chave do KMS, os snapshots serão criptografados usando a chave do KMS padrão de criptografia do EBS em cada região de destino. Se você especificar uma Chave do KMS para a região de destino, a função do IAM selecionada deverá ter acesso à Chave do KMS.

É necessário garantir que o número de cópias de snapshots simultâneas não seja excedido por região.

Se a política criar snapshots em um Outpost, você não poderá copiá-los para uma região ou outro Outpost e as configurações de cópia entre regiões não estarão disponíveis.

6. Em Policy status after creation (Status da política após a criação), selecione Enable policy (Habilitar política) para iniciar as execuções da política no próximo horário agendado ou Disable policy (Desabilitar política) para impedir que a política seja executada.
7. Selecione Create Policy (Criar política).

Command line

Use o comando [create-lifecycle-policy](#) para criar uma política de ciclo de vida de snapshots. Para `PolicyType`, especifique `EBS_SNAPSHOT_MANAGEMENT`.

Note

Para simplificar a sintaxe, os exemplos a seguir usam um arquivo JSON `policyDetails.json`, que inclui os detalhes da política.

Exemplo 1—Política de ciclo de vida de snapshot

Este exemplo cria uma política de ciclo de vida de snapshot que cria snapshots de todos os volumes que têm uma chave de tag de costcenter com um valor de 115. A política inclui duas programações. A primeira programação cria um snapshot todos os dias às 3h UTC. A segunda programação cria um snapshot semanal todas as sextas-feiras às 17h UTC.

```
aws dlm create-lifecycle-policy \  
--description "My volume policy" \  
--state ENABLED --execution-role-arn  
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \  
--policy-details file://policyDetails.json
```

Este é um exemplo do arquivo policyDetails.json.

```
{  
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",  
    "ResourceTypes": [  
        "VOLUME"  
    ],  
    "TargetTags": [{  
        "Key": "costcenter",  
        "Value": "115"  
    }],  
    "Schedules": [{  
        "Name": "DailySnapshots",  
        "TagsToAdd": [{  
            "Key": "type",  
            "Value": "myDailySnapshot"  
        }],  
        "CreateRule": {  
            "Interval": 24,  
            "IntervalUnit": "HOURS",  
            "Times": [  
                "03:00"  
            ]  
        },  
        "RetainRule": {  
            "Count": 5  
        },  
        "CopyTags": false  
    },  
    {  
        "Name": "WeeklySnapshots",  
        "TagsToAdd": [{  
            "Key": "type",  
            "Value": "myWeeklySnapshot"  
        }],  
        "CreateRule": {  
            "CronExpression": "cron(0 17 ? * FRI *)"  
        },  
        "RetainRule": {  
            "Count": 5  
        },  
        "CopyTags": false  
    }]  
}
```

Se for bem-sucedido, o comando retornará o ID da política criada recentemente. A seguir está um exemplo de saída.

```
{  
    "PolicyId": "policy-0123456789abcdef0"  
}
```

Exemplo 2—Política de ciclo de vida de snapshots que automatiza snapshots locais de recursos do Outpost

Este exemplo cria uma política de ciclo de vida de snapshots que cria snapshots de volumes marcados com `team=dev` em todos os seus Outposts. A política cria os snapshots nos mesmos Outposts que os volumes de origem. A política cria snapshots a cada 12 horas a partir das 00:00 UTC.

```
aws dlm create-lifecycle-policy \
--description "My local snapshot policy" \
--state ENABLED --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
--policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",
    "ResourceTypes": "VOLUME",
    "ResourceLocations": "OUTPOST",
    "TargetTags": [
        {
            "Key": "team",
            "Value": "dev"
        }
    ],
    "Schedules": [
        {
            "Name": "on-site backup",
            "CreateRule": {
                "Interval": 12,
                "IntervalUnit": "HOURS",
                "Times": [
                    "00:00"
                ],
                "Location": [
                    "OUTPOST_LOCAL"
                ]
            },
            "RetainRule": {
                "Count": 1
            },
            "CopyTags": false
        }
    ]
}
```

Exemplo 3—A política de ciclo de vida de snapshots que cria snapshots em uma região e os copia para um Outpost

O exemplo de política a seguir cria snapshots de volumes com a tag `team=dev`. Os snapshots são criados na mesma região que o volume de origem. Os snapshots são criados a cada 12 horas a partir das 00:00 UTC e retêm, no máximo, 1 snapshot. A política também copia os snapshots para o Outpost `arn:aws:outposts:us-east-1:123456789012:outpost/op-1234567890abcdef0`, criptografa os snapshots copiados usando a Chave do KMS de criptografia padrão e retém as cópias por 1 mês.

```
aws dlm create-lifecycle-policy \
--description "Copy snapshots to Outpost" \
--state ENABLED --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole \
--policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{  
    "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",  
    "ResourceTypes": "VOLUME",  
    "ResourceLocations": "CLOUD",  
    "TargetTags": [ {  
        "Key": "team",  
        "Value": "dev"  
    } ],  
    "Schedules": [ {  
        "Name": "on-site backup",  
        "CopyTags": false,  
        "CreateRule": {  
            "Interval": 12,  
            "IntervalUnit": "HOURS",  
            "Times": [  
                "00:00"  
            ],  
            "Location": "CLOUD"  
        },  
        "RetainRule": {  
            "Count": 1  
        },  
        "CrossRegionCopyRules" : [  
            {  
                "Target": "arn:aws:outposts:us-east-1:123456789012:outpost/  
op-1234567890abcdef0",  
                "Encrypted": true,  
                "CopyTags": true,  
                "RetainRule": {  
                    "Interval": 1,  
                    "IntervalUnit": "MONTHS"  
                }  
            }  
        ]  
    }  
}
```

Automatizar ciclos de vida da AMI

O procedimento a seguir mostra como usar o Amazon Data Lifecycle Manager para automatizar os ciclos de vida da AMI com suporte do EBS.

Use os procedimentos a seguir para criar uma política de ciclo de vida de AMI.

New console

Para criar uma política de AMI

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Na tela Select policy type (Selecionar tipo de política), escolha EBS-backed AMI policy (Política de AMI com suporte do EBS) e depois Next (Próximo).
4. Na seção Target resources (Recursos de destino), em Target resource tags (Etiquetas de recurso de destino), escolha as etiquetas de recursos que identificam os volumes ou as instâncias dos quais deseja fazer backup. A política só oferece suporte aos recursos que tenham a chave de etiqueta e os pares de valor especificados.
5. Para Description (Descrição), insira uma breve descrição da rota.
6. Em IAM role (Função do IAM), selecione a função do IAM que tem permissões para gerenciar AMIs e snapshots e para descrever instâncias. Para usar a função padrão fornecida pelo Amazon

Data Lifecycle Manager, escolha Default role (Função padrão). Se preferir, para usar uma função do IAM personalizada criada anteriormente, selecione Choose another role (Escolher outra função) e selecione a função a ser usada.

7. Em Policy tags (Etiquetas de políticas), adicione as etiquetas a serem aplicadas na política de ciclo de vida. Você pode usar essas etiquetas para identificar e categorizar suas políticas.
8. Em Policy status after creation (Status da política após a criação), selecione Enable policy (Habilitar política) para iniciar as execuções da política no próximo horário agendado ou Disable policy (Desabilitar política) para impedir que a política seja executada. Se você não habilitar a política agora, ela não começará a criar AMIs até que você a ative manualmente após a criação.
9. Na seção Instance reboot (Reinicialização da instância), indique se as instâncias devem ser reinicializadas antes da criação da AMI. Para evitar que as instâncias de destino sejam reinicializadas, escolha No (Não). Escolher No (Não) pode causar problemas de consistência de dados. Para reiniciar instâncias antes da criação da AMI, escolha Yes (Sim). Escolher isso garante a consistência dos dados, mas pode resultar na reinicialização de várias instâncias direcionadas simultaneamente.
10. Escolha Next (Próximo).
11. Em Configure schedule (Configurar agendamento), configure os agendamentos de política. Uma política pode ter até quatro agendamentos. A Programação 1 é obrigatória. As Programações 2, 3 e 4 são opcionais. Para cada agendamento de política que você adicionar, faça o seguinte:
 - a. Na seção Schedule details (Detalhes do agendamento), faça o seguinte:
 - i. Em Schedule name (Nome do agendamento), especifique um nome descritivo para o agendamento.
 - ii. Em Frequency (Frequência) e nos campos relacionados, configure o intervalo entre as execuções da política. É possível configurar execuções de políticas com uma programação diária, semanal, mensal ou anual. Como opção, escolha Custom cron expression (Expressão cron personalizada) para especificar um intervalo de até 1 ano. Para obter mais informações, consulte [Cron expressions](#) (Expressões cron) no Guia do usuário do Amazon CloudWatch Events.
 - iii. Em Starting at (Iniciando às), especifique a hora para iniciar as execuções da política. A primeira execução da política inicia uma hora depois do horário agendado. É necessário inserir a hora no formato hh:mm UTC.
 - iv. Em Retention type (Tipo de retenção), especifique a política de retenção para AMIs criadas pelo agendamento. Você pode reter AMIs com base na contagem total ou na idade delas.

Para retenção baseada em contagem, o intervalo é de 1 a 1000. Quando a contagem máxima for atingida, a AMI mais antiga será excluída quando uma nova for criada.

Para retenção baseada na idade, o intervalo é de 1 dia a 100 anos. Depois que o período de retenção de cada AMI expirar, ela será excluída.

Note

Todas as programações devem ter o mesmo tipo de retenção. Você pode especificar o tipo de retenção somente para a Programação 1. As Programações 2, 3 e 4 herdam o tipo de retenção da Programação 1. Cada programação pode ter sua própria contagem ou período de retenção.

- b. Na seção Tagging (Marcação), faça o seguinte:
 - i. Para copiar todas as etiquetas definidas por usuário da instância de origem para as AMIs criadas pelo agendamento, selecione Copy tags from source (Copiar etiquetas da origem).
 - ii. Por padrão, as AMIs criadas pelo agendamento são automaticamente marcadas com o ID da instância de origem. Para evitar que essa marcação automática ocorra, em

Variable tags (Etiquetas de variáveis), remova o bloco `instance-id:$(instance-id)`.

- iii. Para especificar etiquetas adicionais a serem atribuídas às AMIs criadas por esse agendamento, escolha Add tags (Adicionar etiquetas).
- c. Para defasar as AMIs quando elas não devem mais ser usadas, na seção Defasagem da AMI, selecione Habilitar a defasagem da AMI para esta programação e, em seguida, especifique a regra de defasagem da AMI. A regra de defasagem da AMI especifica quando as AMIs devem ser defasadas.

Se a programação usar retenção de AMI baseada em contagem, será necessário especificar o número de AMIs mais antigas a serem defasadas. A contagem de defasagem deve ser menor ou igual à contagem de retenção de AMI da programação e não pode ser maior que 1.000. Por exemplo, se a programação estiver configurada para reter no máximo 5 AMIs, você poderá configurar a programação para defasar até 5 das AMIs mais antigas.

Se a programação usar retenção de AMI baseada em idade, será necessário especificar o período após o qual as AMIs serão defasadas. A contagem de defasagem deve ser menor ou igual ao período de retenção da AMI da programação e não pode ser superior a 10 anos (120 meses, 520 semanas ou 3.650 dias). Por exemplo, se a programação estiver configurada para reter AMIs por 10 dias, você poderá configurar a programação para substituir AMIs após períodos de até 10 dias após a criação.

- d. Para copiar AMIs criadas pelo agendamento para regiões diferentes, na seção Cross-Region copy (Cópia entre regiões), selecione Enable cross-Region copy (Habilitar cópia entre regiões). É possível copiar AMIs para até três regiões adicionais em sua conta. Você deve especificar uma regra de cópia entre regiões separada para cada região de destino.

Para cada Região de destino, é possível especificar o seguinte:

- Uma política de retenção para a cópia AMI. Quando o período de retenção expirar, a cópia na Região de destino será automaticamente cancelada.
- Status de criptografia para a cópia da AMI. Se a AMI de origem estiver criptografada ou se a criptografia por padrão estiver habilitada, as AMIs copiadas serão sempre criptografadas. Se a AMI de origem não estiver criptografada e a criptografia por padrão estiver desabilitada, você poderá habilitar a criptografia. Se você não especificar uma chave do KMS, as AMIs serão criptografadas usando a chave do KMS padrão de criptografia do EBS em cada região de destino. Se você especificar uma Chave do KMS para a região de destino, a função do IAM selecionada deverá ter acesso à Chave do KMS.
- Uma regra de defasagem para a cópia da AMI. Quando o período de descontinuação expira, a cópia da AMI é automaticamente substituída. O período de defasagem deve ser menor ou igual ao período de retenção de cópias e não pode ser superior a 10 anos.
- Se deseja copiar todas as marcações ou nenhuma marcação da AMI de origem.

Note

Não exceda o número de cópias de AMI simultâneas por região.

- e. Para adicionar outros agendamentos, escolha Add another schedule (Adicionar outro agendamento), localizado na parte superior da tela. Para cada agendamento adicional, preencha os campos conforme descrito anteriormente neste tópico.
 - f. Depois de adicionar os agendamentos necessárias, escolha Review policy (Revisar política).
12. Revise o resumo da política e escolha Create policy (Criar política).

Console

Para criar uma política de ciclo de vida de AMI

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Forneça as seguintes informações para sua política, conforme necessário:
 - Description (Descrição)—Uma descrição da política.
 - Policy type (Tipo de política)—O tipo de política a ser criada. Selecione EBS-backed AMI policy (Política da AMI com suporte do EBS).
 - Target with these tags (Destino com estas etiquetas): as etiquetas de recursos que identificam as instâncias dos quais fazer backup. A política só oferece suporte às instâncias com a chave de etiqueta e os pares de valor especificados.
 - Lifecycle policy (Política de ciclo de vida): as etiquetas a serem aplicadas à política de ciclo de vida.
4. Em IAM role (função do IAM), escolha a função do IAM que tiver permissões para gerenciar imagens. A AWS fornece uma função padrão, ou você pode criar uma função do IAM personalizada.
5. Adicione as programações de política. A Programação 1 é obrigatória. As Programações 2, 3 e 4 são opcionais. Para cada programação de política que você incluir, especifique as seguintes informações:
 - Schedule name—(Nome da programação): um nome para a programação.
 - Frequency (Frequência)—: o intervalo entre as execuções da política. É possível configurar execuções de políticas com uma programação diária, semanal, mensal ou anual. Como opção, escolha Custom cron expression (Expressão cron personalizada) para especificar um intervalo de até 1 ano. Para obter mais informações, consulte [Cron expressions](#) (Expressões cron) no Guia do usuário do Amazon CloudWatch Events.
 - Starting at hh:mm UTC (Iniciar às hh:mm UTC): a hora em que as execuções da política estão programadas para iniciar. A primeira execução da política começa uma hora depois do horário agendado.
 - Retention type (Tipo de retenção): você pode reter AMIs com base na contagem total ou na idade. Para retenção baseada em contagem, o intervalo é de 1 a 1000. Quando a contagem máxima for atingida, a AMI mais antiga será excluída quando uma nova for criada. Para retenção baseada na idade, o intervalo é de 1 dia a 100 anos. Depois que o período de retenção de cada AMI expirar, ela será excluída. O período de retenção deve ser maior ou igual ao intervalo.

Note

Todas as programações devem ter o mesmo tipo de retenção. Você pode especificar o tipo de retenção somente para a Programação 1. As Programações 2, 3 e 4 herdam o tipo de retenção da Programação 1. Cada programação pode ter sua própria contagem ou período de retenção.

- Copy tags from source (Copiar etiquetas da origem): escolha se deseja copiar todas as etiquetas definidas pelo usuário da instância de origem para as AMIs criadas pelo agendamento.
- Etiquetas dinâmicas: você pode optar por etiquetar automaticamente suas AMIs com o ID da instância de origem.
- Additional tags (Etiquetas adicionais): especifique as etiquetas adicionais a serem atribuídas às AMIs criadas por esse agendamento.
- Enable cross Region copy (Habilitar cópia entre regiões): é possível copiar AMIs para até três regiões adicionais.

Para cada região, é possível escolher diferentes políticas de retenção e se deseja copiar todas as tags ou nenhuma tag. Se a AMI de origem estiver criptografada ou se a criptografia por padrão estiver habilitada, as AMIs copiadas serão criptografadas. Se a AMI não estiver criptografada, você poderá habilitar a criptografia. Se você não especificar uma chave do KMS, as AMIs serão criptografadas usando a chave do KMS padrão de criptografia do EBS em cada região de destino. Se você especificar uma Chave do KMS para a região de destino, a função do IAM selecionada deverá ter acesso à Chave do KMS.

Não exceda o número de cópias de AMI simultâneas por região.

6. Indique se as instâncias devem ser reinicializadas antes da criação da AMI. Para evitar que as instâncias de destino sejam reinicializadas, para Reboot Instance at policy run (Reiniciar Instância na execução da política) escolha No (Não). A escolha dessa opção pode causar problemas de consistência de dados. Para reiniciar instâncias antes da criação da AMI, para Reboot Instance at policy run (Reiniciar Instância na execução da política), escolha Yes (Sim). Escolher isso garante a consistência dos dados, mas pode resultar na reinicialização de várias instâncias direcionadas simultaneamente.
7. Em Policy status after creation (Status da política após a criação), selecione Enable policy (Habilitar política) para iniciar as execuções da política no próximo horário agendado ou Disable policy (Desabilitar política) para impedir que a política seja executada.
8. Selecione Create Policy (Criar política).

Command line

Use o comando [create-lifecycle-policy](#) para criar uma política de ciclo de vida de AMI. Para PolicyType, especifique IMAGE_MANAGEMENT.

Note

Para simplificar a sintaxe, os exemplos a seguir usam um arquivo JSON policyDetails.json, que inclui os detalhes da política.

Exemplo 1: retenção baseada em idade e defasagem de AMI

Esse exemplo cria uma política de ciclo de vida da AMI que cria AMIs de todas as instâncias que têm uma chave de marcação purpose com um valor de production e reinicia as instâncias direcionadas. A política inclui uma programação que cria uma AMI todos os dias às 01:00 UTC. A política mantém AMIs por 2 dias e faz a defasagem depois de 1 dia. Também copia as etiquetas da instância de origem para as AMIs criadas por ela.

```
aws dlm create-lifecycle-policy \
--description "My AMI policy" \
--state ENABLED --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \
--policy-details file://policyDetails.json
```

Este é um exemplo do arquivo policyDetails.json.

```
{
    "PolicyType": "IMAGE_MANAGEMENT",
    "ResourceTypes": [
        "INSTANCE"
    ],
    "TargetTags": [
        {
            "Key": "purpose",
            "Value": "production"
        }
    ],
    "Schedules": [
        {
            "Name": "DailyAMIS",
            "Schedule": "cron(0 1 * * *)"
        }
    ]
}
```

```
"TagsToAdd": [{  
    "Key": "type",  
    "Value": "myDailyAMI"  
}],  
"CreateRule": {  
    "Interval": 24,  
    "IntervalUnit": "HOURS",  
    "Times": [  
        "01:00"  
    ]  
},  
"RetainRule":{  
    "Interval" : 2,  
    "IntervalUnit" : "DAYS"  
},  
"DeprecateRule": {  
    "Interval" : 1,  
    "IntervalUnit" : "DAYS"  
},  
"CopyTags": true  
}  
],  
"Parameters" : {  
    "NoReboot":true  
}  
}
```

Se for bem-sucedido, o comando retornará o ID da política criada recentemente. A seguir está um exemplo de saída.

```
{  
    "PolicyId": "policy-9876543210abcdef0"  
}
```

Exemplo 2: retenção baseada em contagem e defasagem de AMI com cópia entre Regiões

Esse exemplo cria uma política de ciclo de vida da AMI que cria AMIs de todas as instâncias que têm uma chave de marcação `purpose` com um valor de `production` e reinicializa as instâncias direcionadas. A política inclui uma programação que cria uma AMI a cada 6 horas a partir de 17:30 UTC. A política retém AMIs 3 e faz a defasagem automaticamente de 2 AMIs mais antigas. Ela também tem uma regra de cópia entre Regiões que copia AMIs para `us-east-1`, mantém 2 cópias de AMI e faz a defasagem automaticamente da AMI mais antiga.

```
aws dlm create-lifecycle-policy \  
--description "My AMI policy" \  
--state ENABLED \  
--execution-role-arn  
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRoleForAMIManagement \  
--policy-details file://policyDetails.json
```

Este é um exemplo do arquivo `policyDetails.json`.

```
{  
    "PolicyType": "IMAGE_MANAGEMENT",  
    "ResourceTypes" : [  
        "INSTANCE"  
    ],  
    "TargetTags": [{  
        "Key": "purpose",  
        "Value": "production"  
    }],
```

```
"Parameters" : {  
    "NoReboot": true  
},  
"Schedules" : [{  
    "Name" : "Schedule1",  
    "CopyTags": true,  
    "CreateRule" : {  
        "Interval": 6,  
        "IntervalUnit": "HOURS",  
        "Times" : ["17:30"]  
    },  
    "RetainRule":{  
        "Count" : 3  
    },  
    "DeprecateRule":{  
        "Count" : 2  
    },  
    "CrossRegionCopyRules": [{  
        "TargetRegion": "us-east-1",  
        "Encrypted": true,  
        "RetainRule":{  
            "IntervalUnit": "DAYS",  
            "Interval": 2  
        },  
        "DeprecateRule":{  
            "IntervalUnit": "DAYS",  
            "Interval": 1  
        },  
        "CopyTags": true  
    }]  
}]  
}
```

Automatizar cópias de snapshots entre contas

A automatização de cópias de snapshots entre contas permite copiar seus snapshots do Amazon EBS para regiões específicas em uma conta isolada e criptografar esses snapshots com uma chave de criptografia. Isso permite que você se proteja contra perda de dados no caso de sua conta ser comprometida.

A automatização de cópias de snapshots entre contas envolve duas contas:

- Conta de origem—A conta de origem é a conta que cria e compartilha os snapshots com a conta de destino. Nesta conta, você deve criar uma política de snapshot do EBS que crie snapshots em intervalos definidos e compartilhe-os com outras contas da AWS.
- Conta de destino—A conta de destino é a conta com a conta de destino com a qual os snapshots são compartilhados e é a conta que cria cópias dos instantâneos compartilhados. Nesta conta, você deve criar uma política de eventos de cópia entre contas que copia automaticamente snapshots compartilhados com ela por uma ou mais contas de origem especificadas.

Tópicos

- [Criar políticas de cópia de snapshot entre contas \(p. 1382\)](#)
- [Especificar filtros de descrição de snapshot \(p. 1390\)](#)

Criar políticas de cópia de snapshot entre contas

Para preparar as contas de origem e de destino para cópia de snapshot entre contas, você precisa executar as seguintes etapas:

Tópicos

- [Etapa 1: Criar a política de snapshot do EBS \(conta de origem\) \(p. 1383\)](#)
- [Etapa 2: Compartilhe a chave gerenciada pelo cliente \(Conta de origem\) \(p. 1383\)](#)
- [Etapa 3: criar política de eventos de cópia entre contas \(conta de destino\) \(p. 1385\)](#)
- [Etapa 4: permitir que a função do IAM use as Chaves do KMS necessárias \(conta de destino\) \(p. 1388\)](#)

[Etapa 1: Criar a política de snapshot do EBS \(conta de origem\)](#)

Na conta de origem, crie uma política de snapshot do EBS que criará os snapshots e os compartilhará com as contas de destino necessárias.

Ao criar a política, certifique-se de habilitar o compartilhamento entre contas e especificar as contas da AWS de destino com as quais os snapshots serão compartilhados. Estas são as contas com as quais os snapshots devem ser compartilhados. Se você estiver compartilhando snapshots criptografados, deverá dar permissão às contas de destino selecionadas para usar a Chave do KMS usada para criptografar o volume de origem. Para obter mais informações, consulte [Etapa 2: Compartilhe a chave gerenciada pelo cliente \(Conta de origem\) \(p. 1383\)](#).

Para obter mais informações sobre como criar um snapshot de política do EBS, consulte [Automação dos ciclos de vida do snapshot \(p. 1368\)](#).

Use um dos métodos a seguir para criar a política de snapshot do EBS.

[Etapa 2: Compartilhe a chave gerenciada pelo cliente \(Conta de origem\)](#)

Se você estiver compartilhando snapshots criptografados, você deve conceder a função do IAM e as contas da AWS de destino (que você selecionou na etapa anterior) permissões para usar a chave gerenciada pelo cliente que foi usada para criptografar o volume de origem.

Note

Execute esta etapa apenas se você estiver compartilhando snapshots criptografados. Se você estiver compartilhando snapshots não criptografados, pule esta etapa.

Console

1. Abra o console do AWS KMS em <https://console.aws.amazon.com/kms>.
2. Para alterar a região da AWS, use o Region selector (Seletor de regiões) no canto superior direito da página.
3. No painel de navegação, escolha Customer managed key (Chave gerenciadas pelo cliente) e selecione a chave do KMS que você precisa compartilhar com as contas de destino.

Anote o ARN da Chave do KMS, você precisará disso mais tarde.

4. Na guia Key policy (Política de chave), role para baixo até a seção Key users (Usuários chave). Escolha Add (Adicionar), insira o nome da função do IAM que você selecionou na etapa anterior e escolha Add (Adicionar).
5. Na guia Key policy (Política de chave), role para baixo até a seção Other AWS accounts (Outras contas da AWS). Escolha Add other AWS accounts (Adicionar outras contas da AWS) e, em seguida, adicione todas as contas da AWS de destino com as quais você escolheu compartilhar os snapshots na etapa anterior.
6. Selecione Save changes (Salvar alterações).

Command line

Use o comando [get-key-policy](#) para recuperar a política de chaves que está atualmente vinculada à Chave do KMS.

Por exemplo, o comando a seguir recupera a política de chaves para uma Chave do KMS com um ID de 9d5e2b3d-e410-4a27-a958-19e220d83a1e e a grava em um arquivo chamado `snapshotKey.json`.

```
$ aws kms get-key-policy \
--policy-name default --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e \
--query Policy --output text > snapshotKey.json
```

Abra a política de chaves usando seu editor de texto preferido. Adicione o ARN da função do IAM que você especificou quando criou a política de snapshot e os ARNs das contas de destino com as quais deseja compartilhar a Chave do KMS.

Por exemplo, na política a seguir, adicionamos o ARN da função padrão do IAM e o ARN da conta raiz da conta de destino 222222222222.

```
{
    "Sid" : "Allow use of the key",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource" : "*"
},
{
    "Sid" : "Allow attachment of persistent resources",
    "Effect" : "Allow",
    "Principal" : {
        "AWS" : [
            "arn:aws:iam::111111111111:role/service-role/
AWSDataLifecycleManagerDefaultRole",
            "arn:aws:iam::222222222222:root"
        ]
    },
    "Action" : [
        "kms>CreateGrant",
        "kms>ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource" : "*",
    "Condition" : {
        "Bool" : {
            "kms:GrantIsForAWSResource" : "true"
        }
    }
}
```

Salve e feche o arquivo . Use então o comando [put-key-policy](#) para anexar a política chave atualizada à Chave do KMS.

```
$ aws kms put-key-policy \
--policy-name default --key-id 9d5e2b3d-e410-4a27-a958-19e220d83a1e
--policy file://snapshotKey.json
```

Etapa 3: criar política de eventos de cópia entre contas (conta de destino)

Na conta de destino, você deve criar uma política de eventos de cópia entre contas que copiará automaticamente os snapshots compartilhados pelas contas de origem necessárias.

Essa política só é executada na conta de destino quando uma das contas de origem especificadas compartilha o snapshot com a conta.

Use um dos seguintes métodos para criar a política de eventos de cópia entre contas.

New console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Elastic Block Store, Lifecycle Manager ((Gerenciador de ciclo de vida) e Create snapshot lifecycle policy (Criar política de ciclo de vida de snapshot).
3. Na tela Select policy type (Selecionar tipo de política), escolha Cross-account copy event policy (Cópia de política de eventos entre contas) e depois Next (Próximo).
4. Em Policy description (Descrição da política), insira uma breve descrição da política.
5. Em Policy tags (Etiquetas de políticas), adicione as etiquetas a serem aplicadas na política de ciclo de vida. Você pode usar essas etiquetas para identificar e categorizar suas políticas.
6. Na seção Event settings (Configurações de evento), defina o evento de compartilhamento de snapshots que fará com que a política seja executada. Faça o seguinte:
 - a. Em Sharing accounts (Compartilhando contas), especifique as contas da AWS de origem das quais você deseja copiar os snapshots compartilhados. Selecione Add account (Adicionar conta), insira o ID de 12 dígitos da conta da AWS e escolha Add (Adicionar).
 - b. Em Filter by description (Filtrar por descrição), insira a descrição necessária do snapshot usando uma expressão regular. Somente os snapshots que são compartilhados pelas contas de origem especificadas e que tenham descrições que correspondam ao filtro especificado são copiados pela política. Para obter mais informações, consulte [Especificar filtros de descrição de snapshot \(p. 1390\)](#).
7. Para a IAM role (função do IAM), escolha a função do IAM que tem permissões para executar ações de cópia de snapshots. Para usar a função padrão fornecida pelo Amazon Data Lifecycle Manager, escolha Default role (Função padrão). Se preferir, para usar uma função do IAM personalizada criada anteriormente, selecione Choose another role (Escolher outra função) e selecione a função a ser usada.

Se você estiver copiando snapshots criptografados, você deve conceder as permissões de função do IAM selecionadas para usar a Chave do KMS de criptografia usada para criptografar o volume de origem. Da mesma forma, se você estiver criptografando o snapshot na região de destino usando uma Chave do KMS diferente, deverá conceder a permissão de função do IAM para usar a Chave do KMS de destino. Para obter mais informações, consulte [Etapa 4: permitir que a função do IAM use as Chaves do KMS necessárias \(conta de destino\) \(p. 1388\)](#).

8. Na seção Copy action (Copiar ação), defina as ações de cópia de snapshots que a política deve executar quando for ativada. A política pode copiar snapshots para até três regiões. Você deve especificar uma regra de cópia separada para cada região de destino. Para cada regra que você adicionar, faça o seguinte:

- a. Para Name (Nome), insira um nome descritivo para a ação de cópia.
- b. Em Target Region (Região de destino), selecione a região para a qual deseja copiar os snapshots.
- c. Em Expire, especifique por quanto tempo manter as cópias de snapshot na região de destino após a criação.
- d. Para criptografar a cópia do snapshot, Em Encryption (Criptografia), selecione Enable encryption (Habilitar criptografia). Se o snapshot de origem estiver criptografado ou se a criptografia por padrão estiver habilitada para a sua conta, a cópia do snapshot será sempre criptografada, mesmo que você não habilite a criptografia aqui. Se o snapshot de origem não estiver criptografado e a criptografia por padrão não estiver habilitada para sua conta, você poderá optar por ativar ou desativar a criptografia. Se você habilitar a criptografia, mas não especificar uma Chave do KMS, os snapshots serão criptografados usando a Chave do KMS de criptografia padrão em cada região de destino. Se você especificar uma Chave do KMS para a região de destino, deverá ter acesso à Chave do KMS.
9. Para adicionar outras ações de cópia de snapshot, escolha Add New Regions (Adicionar novas regiões).
10. Em Policy status after creation (Status da política após a criação), selecione Enable policy (Habilitar política) para iniciar as execuções da política no próximo horário agendado ou Disable policy (Desabilitar política) para impedir que a política seja executada. Se você não habilitar a política agora, ela não começará a copiar snapshots até que você a ative manualmente após a criação.
11. Escolha Create policy (Criar política).

Old console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Lifecycle Manager (Gerenciador de ciclo de vida) e escolha Create Lifecycle Policy (Criar política de ciclo de vida).
3. Para Policy Type (Tipo de Política), escolha Cross-account copy event policy (Política de eventos de cópia entre contas). Para Description (Descrição), insira uma breve descrição da rota.
4. Na seção Cross-account copy event settings (Configurações de eventos de cópia entre contas), para Copy snapshots shared by (Copiar instantâneos compartilhados por), insira as contas da AWS de origem a partir das quais você deseja copiar os snapshots compartilhados.
5. Para Snapshot description filter (Filtro de descrição do snapshot), insira a descrição necessária do snapshot usando uma expressão regular. Somente os snapshots que são compartilhados pelas contas de fontes especificadas e que tenham descrições que correspondam ao filtro especificado são copiados pela política. Para obter mais informações, consulte [Especificar filtros de descrição de snapshot \(p. 1390\)](#).
6. Para a função do IAM, escolha a que tiver permissões para executar a ação de cópia de snapshot. A AWS fornece uma função padrão ou você pode criar uma função do IAM personalizada.

Se você estiver copiando snapshots criptografados, você deve conceder as permissões de função do IAM selecionadas para usar a Chave do KMS de criptografia usada para criptografar o volume de origem. Da mesma forma, se você estiver criptografando o snapshot na região de destino usando uma Chave do KMS diferente, deverá conceder a permissão de função do IAM para usar a Chave do KMS de destino. Para obter mais informações, consulte [Etapa 4: permitir que a função do IAM use as Chaves do KMS necessárias \(conta de destino\) \(p. 1388\)](#).

7. Na seção Copy settings (Copiar configurações), você pode configurar a política para copiar snapshots para até três regiões na conta de destino. Faça o seguinte:
 - a. Para Name (Nome), insira um nome descritivo para a ação de cópia.

- b. Em Target Region (Região de destino), selecione a região para a qual deseja copiar os snapshots.
 - c. Para Retain copy for (Reter cópia para), especifique por quanto tempo manter as cópias de snapshot na região de destino após a criação.
 - d. Em Encryption (Criptografia), selecione Enable (Ativar) para criptografar a cópia do snapshot na região de destino. Se o snapshot de origem estiver criptografado ou se a criptografia por padrão estiver habilitada para sua conta, a cópia do snapshot será sempre criptografada, mesmo que você não habilite a criptografia aqui. Se o snapshot de origem não estiver criptografado e a criptografia por padrão não estiver habilitada para sua conta, você poderá optar por ativar ou desativar a criptografia. Se você habilitar a criptografia, mas não especificar uma Chave do KMS, os snapshots serão criptografados usando a Chave do KMS de criptografia padrão em cada região de destino. Se você especificar uma Chave do KMS para a região de destino, deverá ter acesso à Chave do KMS.
 - e. (Opcional) Para copiar o snapshot para regiões adicionais, escolha Add additional region (Adicionar região adicional) e preencha os campos obrigatórios.
8. Para o Policy status after creation (Status da política após a criação), escolha Enable policy (Ativar política) para iniciar as execuções da política na próxima hora programada.
 9. Selecione Create Policy (Criar política).

Command line

Use o comando [create-lifecycle-policy](#) para criar uma política de ciclo de vida. Para criar uma política de eventos de cópia entre contas, para **PolicyType**, especifique **EVENT_BASED_POLICY**.

Por exemplo, o comando a seguir cria uma política de eventos de cópia entre contas na conta de destino 222222222222. A política copia snapshots que são compartilhados pela conta de origem 111111111111. A política copia snapshots para sa-east-1 e eu-west-2. Os snapshots copiados para sa-east-1 são criptografados e retidos por 3 dias. Os snapshots copiados para eu-west-2 são criptografados usando a Chave do KMS 8af79514-350d-4c52-bac8-8985e84171c7 e são retidos por 1 mês. A política usa a função padrão do IAM.

```
$ aws dlm create-lifecycle-policy \
--description "Copy policy" \
--state ENABLED --execution-role-arn arn:aws:iam::222222222222:role/service-role/
AWSDataLifecycleManagerDefaultRole \
--policy-details file://policyDetails.json
```

O exemplo a seguir mostra o conteúdo de um arquivo **policyDetails.json**.

```
{
    "PolicyType" : "EVENT_BASED_POLICY",
    "EventSource" : {
        "Type" : "MANAGED_CWE",
        "Parameters": {
            "EventType" : "shareSnapshot",
            "SnapshotOwner": ["111111111111"]
        }
    },
    "Actions" : [
        {
            "Name" :"Copy Snapshot to Sao Paulo and London",
            "CrossRegionCopy" : [
                {
                    "Target" : "sa-east-1",
                    "EncryptionConfiguration" : {
                        "Encrypted" : false
                    },
                    "RetainRule" : {
                        "Interval" : 3,
                        "Count" : 1
                    }
                },
                {
                    "Target" : "eu-west-2",
                    "EncryptionConfiguration" : {
                        "Encrypted" : true
                    },
                    "RetainRule" : {
                        "Interval" : 1,
                        "Count" : 1
                    }
                }
            ]
        }
    ]
}
```

```
        "IntervalUnit" : "DAYS"
    }
},
{
    "Target" : "eu-west-2",
    "EncryptionConfiguration" : {
        "Encrypted" : true,
        "CmkArn" : "arn:aws:kms:eu-west-2:222222222222:key/8af79514-350d-4c52-
bac8-8985e84171c7"
    },
    "RetainRule" : {
        "Interval" : 1,
        "IntervalUnit" : "MONTHS"
    }
}
]
```

Se for bem-sucedido, o comando retornará o ID da política criada recentemente. A seguir está um exemplo de saída.

```
{
    "PolicyId": "policy-9876543210abcdef0"
}
```

Etapa 4: permitir que a função do IAM use as Chaves do KMS necessárias (conta de destino)

Se você estiver copiando snapshots criptografados, deverá conceder à função do IAM (que você selecionou na etapa anterior) permissões para usar a chave gerenciada pelo cliente que foi usada para criptografar o volume de origem.

Note

Execute esta etapa somente se você estiver copiando snapshots criptografados. Se você estiver copiando snapshots não criptografados, ignore esta etapa.

Use um dos métodos a seguir para adicionar as políticas necessárias à função do IAM.

Console

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, selecione Settings (Configurações). Pesquise e selecione a função do IAM selecionada ao criar a política de eventos de cópia entre contas na etapa anterior. Se você optou por usar a função padrão, a função será nomeada AWSDataLifecycleManagerDefaultRole.
3. Escolha Add inline policy (Adicionar política em linha) e, em seguida, a guia JSON.
4. Substitua a política existente pelo seguinte e especifique os ARNs das Chaves do KMS:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:RevokeGrant",
                "kms>CreateGrant",
                "kms>ListGrants"
            ],
            "Resource": [

```

```
        "arn:aws:kms:region:source_account_id:key/shared_cmk_id",
        "arn:aws:kms:region:source_account_id:key/shared_cmk_id"
    ],
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": [
        "arn:aws:kms:region:source_account_id:key/shared_cmk_id",
        "arn:aws:kms:region:source_account_id:key/shared_cmk_id"
    ]
}
]
```

5. Escolha Review policy (Revisar política)
6. Para Name (Nome), insira um nome descriptivo para a política e escolha Create policy (Criar política).

Command line

Usando seu editor de texto preferido, crie um novo arquivo JSON chamado `policyDetails.json`. Adicione a política a seguir e especifique os ARNs das Chaves do KMS que a função precisa de permissões para usar. No exemplo a seguir, a política concede a permissão de função do IAM para usar a Chave do KMS1234abcd-12ab-34cd-56ef-1234567890ab, que foi compartilhada pela conta de origem 111111111111 e Chave do KMS4567dcba-23ab-34cd-56ef-0987654321yz que existem na conta de destino 222222222222.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:RevokeGrant",
                "kms>CreateGrant",
                "kms>ListGrants"
            ],
            "Resource": [
                "arn:aws:kms:sa-
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "arn:aws:kms:eu-
west-2:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:region:source_account_id:key/shared_cmk_id",
                "arn:aws:kms:region:source_account_id:key/shared_cmk_id"
            ]
        }
    ]
}
```

```
"Action": [  
    "kms:Encrypt",  
    "kms:Decrypt",  
    "kms:ReEncrypt*",  
    "kms:GenerateDataKey*",  
    "kms:DescribeKey"  
],  
"Resource": [  
    "arn:aws:kms:sa-  
east-1:111111111111:key/1234abcd-12ab-34cd-56ef-1234567890ab",  
    "arn:aws:kms:eu-  
west-2:222222222222:key/4567dcba-23ab-34cd-56ef-0987654321yz"  
]  
}  
}]  
}
```

Salve e feche o arquivo . Em seguida, use o comando [put-role-policy](#) para adicionar a política à função do IAM.

Por exemplo

```
$ aws iam put-role-policy \  
--role-name AWSDataLifecycleManagerDefaultRole \  
--policy-name CopyPolicy \  
--policy-document file://AdminPolicy.json
```

Especificar filtros de descrição de snapshot

Quando você cria a política de cópia de snapshot na conta de destino, você deve especificar um filtro de descrição de snapshot. O filtro de descrição do snapshot permite especificar um nível adicional de filtragem que permite controlar quais snapshots são copiados pela política. Isso significa que um snapshot só será copiado pela política se for compartilhado por uma das contas de origem especificadas e tiver uma descrição de snapshot que corresponda ao filtro especificado. Em outras palavras, se um snapshot for compartilhado por uma das contas de destino especificadas, mas não tiver uma descrição que corresponda ao filtro especificado, ele não será copiado pela política.

A descrição do filtro de snapshot deve ser especificada usando uma expressão regular. É um campo obrigatório ao criar políticas de eventos de cópia entre contas usando o console e a linha de comando. A seguir estão exemplos de expressões regulares que podem ser usadas:

- .*—Esse filtro corresponde a todas as descrições de snapshot. Se você usar essa expressão, a política copiará todos os snapshots compartilhados por uma das contas de origem especificadas.
- Created for policy: policy-0123456789abcdef0.*—Este filtro corresponde apenas aos snapshots criados por uma política com um ID de policy-0123456789abcdef0. Se você usar uma expressão como esta, apenas snapshots que são compartilhados com sua conta por uma das contas de origem especificadas e que foram criados por uma política com o ID especificado serão copiados pela política.
- .*production.*—Esse filtro corresponde a qualquer snapshot que tenha a palavra production em qualquer lugar em sua descrição. Se você usar essa expressão, a política copiará todos os snapshots compartilhados por uma das contas de origem especificadas e que tenham o texto especificado em sua descrição.

Exibir, modificar e excluir políticas de ciclo de vida

Use os procedimentos a seguir para exibir, modificar e excluir políticas de ciclo de vida existentes.

Tópicos

- [Visualizar políticas de ciclo de vida \(p. 1391\)](#)
- [Modificar políticas de ciclo de vida \(p. 1392\)](#)
- [Excluir políticas de ciclo de vida \(p. 1393\)](#)

Visualizar políticas de ciclo de vida

Use um dos procedimentos a seguir para exibir uma política de ciclo de vida.

Console

Como exibir uma política de ciclo de vida

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic Block Store e, depois, Lifecycle Manager (Gerenciador de ciclo de vida).
3. Selecione uma política de ciclo de vida na lista. A guia Details (Detalhes) exibe as seguintes informações sobre a política.

Command line

Use o comando `get-lifecycle-policy` para exibir informações sobre uma política de ciclo de vida.

```
aws dlm get-lifecycle-policy --policy-id policy-0123456789abcdef0
```

A seguir está um exemplo de saída. Ele inclui as informações que você especificou, além dos metadados inseridos pela AWS.

```
{  
    "Policy": {  
        "Description": "My first policy",  
        "DateCreated": "2018-05-15T00:16:21+0000",  
        "State": "ENABLED",  
        "ExecutionRoleArn":  
            "arn:aws:iam::210774411744:role/AWSDataLifecycleManagerDefaultRole",  
        "PolicyId": "policy-0123456789abcdef0",  
        "DateModified": "2018-05-15T00:16:22+0000",  
        "PolicyDetails": {  
            "PolicyType": "EBS_SNAPSHOT_MANAGEMENT",  
            "ResourceTypes": [  
                "VOLUME"  
            ],  
            "TargetTags": [  
                {  
                    "Value": "115",  
                    "Key": "costcenter"  
                }  
            ],  
            "Schedules": [  
                {  
                    "TagsToAdd": [  
                        {  
                            "Value": "myDailySnapshot",  
                            "Key": "type"  
                        }  
                    ],  
                    "RetainRule": {  
                        "Count": 1,  
                        "Unit": "Days"  
                    }  
                }  
            ]  
        }  
    }  
}
```

```
        "Count": 5
    },
    "CopyTags": false,
    "CreateRule": {
        "Interval": 24,
        "IntervalUnit": "HOURS",
        "Times": [
            "03:00"
        ]
    },
    "Name": "DailySnapshots"
}
]
}
}
```

Modificar políticas de ciclo de vida

Use um dos procedimentos a seguir para modificar uma política de ciclo de vida.

Console

Para modificar uma política de ciclo de vida

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic Block Store e, depois, Lifecycle Manager (Gerenciador de ciclo de vida).
3. Selecione uma política de ciclo de vida na lista.
4. Escolha Actions (Ações), Modify Lifecycle Policy (Modificar Política de Ciclo de Vida).
5. Modifique as configurações da política, conforme necessário. Por exemplo, é possível modificar a programação, adicionar ou remover tags ou habilitar e desabilitar a política.
6. Escolha Update policy.

Command line

Use o comando `update-lifecycle-policy` para modificar informações em uma política de ciclo de vida. Para simplificar a sintaxe, este exemplo faz referência ao arquivo JSON `policyDetailsUpdated.json` que inclui os detalhes da política.

```
aws dlm update-lifecycle-policy --state DISABLED --execution-role-arn
arn:aws:iam::12345678910:role/AWSDataLifecycleManagerDefaultRole" --policy-details
file://policyDetailsUpdated.json
```

Este é um exemplo do arquivo `policyDetailsUpdated.json`.

```
{
    "ResourceTypes": [
        "VOLUME"
    ],
    "TargetTags": [
        {
            "Key": "costcenter",
            "Value": "120"
        }
    ],
}
```

```
"Schedules": [
    {
        "Name": "DailySnapshots",
        "TagsToAdd": [
            {
                "Key": "type",
                "Value": "myDailySnapshot"
            }
        ],
        "CreateRule": {
            "Interval": 12,
            "IntervalUnit": "HOURS",
            "Times": [
                "15:00"
            ]
        },
        "RetainRule": {
            "Count": 5
        },
        "CopyTags": false
    }
]
```

Para visualizar a política atualizada, use o comando `get-lifecycle-policy`. Você pode ver que o estado, o valor da tag, o intervalo de snapshots e o horário de início do snapshot foram alterados.

Excluir políticas de ciclo de vida

Use um dos procedimentos a seguir para excluir uma política de ciclo de vida.

Note

Quando você exclui uma política de ciclo de vida, os snapshots ou AMIs criados por essa política não são excluídos automaticamente. Se não precisar mais dos snapshots ou AMIs, você deve excluí-los manualmente.

Old console

Para excluir uma política de ciclo de vida

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Elastic Block Store e, depois, Lifecycle Manager (Gerenciador de ciclo de vida).
3. Selecione uma política de ciclo de vida na lista.
4. Escolha Actions (Ações), Delete Lifecycle Policy (Excluir política de ciclo de vida).
5. Quando solicitado por confirmação, escolha Delete Snapshot Lifecycle Policy (Excluir política de ciclo de vida de snapshots).

Command line

Use o comando `delete-lifecycle-policy` para excluir uma política de ciclo de vida e liberar as tag de destino especificadas na política para reutilização.

Note

Você pode excluir snapshots criados somente por Amazon Data Lifecycle Manager.

```
aws dlm delete-lifecycle-policy --policy-id policy-0123456789abcdef0
```

A Referência de API do Amazon Data Lifecycle Manager fornece as descrições e a sintaxe de cada uma das ações e dos tipos de dados para a API de consulta do Amazon Data Lifecycle Manager.

Como alternativa, você pode usar um dos AWS SDKs para acessar a API de uma maneira que seja personalizada para a linguagem de programação ou a plataforma que você estiver usando. Para obter mais informações, consulte [AWS SDKs](#).

AWS Identity and Access Management

O acesso ao Amazon Data Lifecycle Manager exige credenciais. Essas credenciais devem ter permissões para acessar os recursos AWS, como instâncias, volumes, snapshots e AMIs. As seções a seguir fornecem detalhes sobre como você pode usar o AWS Identity and Access Management (IAM) e ajudar a garantir o acesso aos recursos.

Tópicos

- AWSPolíticas gerenciadas pela (p. 1394)
 - Funções de serviço da IAM (p. 1397)
 - Permissões para usuários do IAM (p. 1399)
 - Permissões para criptografia (p. 1400)

AWSPolíticas gerenciadas pela

Uma política gerenciada AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas AWS são criadas para fornecer permissões para vários casos de uso comuns. As políticas gerenciadas AWS tornam mais eficiente a atribuição de permissões apropriadas a usuários, grupos e funções do que se você tivesse que elaborar suas próprias políticas.

Porém, você não pode alterar as permissões definidas em políticas gerenciadas AWS. Ocasionalmente, a AWS atualiza as permissões definidas em uma política gerenciada AWS. Quando isso ocorre, a atualização afetará todas as principais entidades (usuários, grupos e funções) às quais a política está anexada.

O Amazon Data Lifecycle Manager oferece duas políticas gerenciadas AWS para casos de uso comuns. Essas políticas tornam mais eficiente definir as permissões apropriadas e controlar o acesso aos seus recursos. As políticas gerenciadas AWS fornecidas pelo Amazon Data Lifecycle Manager foram projetadas para serem anexadas às funções que você transmitir ao Amazon Data Lifecycle Manager.

Seguem exemplos de políticas gerenciadas AWS fornecidas pelo Amazon Data Lifecycle Manager. Você pode encontrar essas políticas gerenciadas AWS na seção Políticas do console IAM.

AWSDataLifecycleManagerServiceRole

A política AWSDataLifecycleClemanagerServiceRole fornece permissões apropriadas para o Amazon Data Lifecycle Manager criar e gerenciar políticas de snapshots do Amazon EBS e políticas de eventos de cópia entre contas.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateSnapshot",
```

```
"ec2:CreateSnapshots",
"ec2>DeleteSnapshot",
"ec2:DescribeInstances",
"ec2:DescribeVolumes",
"ec2:DescribeSnapshots",
"ec2:EnableFastSnapshotRestores",
"ec2:DescribeFastSnapshotRestores",
"ec2:DisableFastSnapshotRestores",
"ec2:CopySnapshot",
"ec2:ModifySnapshotAttribute",
"ec2:DescribeSnapshotAttribute"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
"ec2>CreateTags"
],
"Resource": "arn:aws:ec2:::snapshot/*"
},
{
"Effect": "Allow",
"Action": [
"events:PutRule",
"events:DeleteRule",
"events:DescribeRule",
"events:EnableRule",
"events:DisableRule",
"events>ListTargetsByRule",
"events:PutTargets",
"events:RemoveTargets"
],
"Resource": "arn:aws:events::rule/AwsDataLifecycleRule.managed-cwe.*"
}
]
}
```

AWSDataLifecycleManagerServiceRoleForAMIManagement

A política AWSDataLifecycleManagerServiceRoleForAMIManagement oferece permissões apropriadas ao Amazon Data Lifecycle Manager para criar e gerenciar políticas da AMI baseada no Amazon EBS.

```
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "ec2>CreateTags",
"Resource": [
"arn:aws:ec2:::snapshot/*",
"arn:aws:ec2:::image/*"
]
},
{
"Effect": "Allow",
"Action": [
"ec2:DescribeImages",
"ec2:DescribeInstances",
"ec2:DescribeImageAttribute",
"ec2:DescribeVolumes",
"ec2:DescribeSnapshots",
"ec2:EnableImageDeprecation",
"ec2:DisableImageDeprecation"
]
```

```
        ],
        "Resource": "*"
    },
{
    "Effect": "Allow",
    "Action": "ec2>DeleteSnapshot",
    "Resource": "arn:aws:ec2:*::snapshot/*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:ResetImageAttribute",
        "ec2:DeregisterImage",
        "ec2>CreateImage",
        "ec2:CopyImage",
        "ec2:ModifyImageAttribute"
    ],
    "Resource": "*"
}
]
```

Atualização da política gerenciada AWS

Os serviços da AWS mantêm e atualizam políticas gerenciadas pela AWS. Não é possível alterar as permissões em políticas gerenciadas pela AWS. Os serviços ocasionalmente acrescentam permissões adicionais a uma política gerenciada pela AWS para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política gerenciada pela AWS quando um novo recurso for iniciado ou novas operações se tornarem disponíveis. Os serviços não removem permissões de uma política gerenciada pela AWS, portanto, as atualizações de políticas não suspendem suas permissões existentes.

A tabela a seguir fornece detalhes as atualizações em políticas gerenciadas AWS para o Amazon Data Lifecycle Manager desde que esse serviço começou a rastrear essas alterações. Para obter alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS em [Histórico do documento \(p. 1704\)](#).

Alteração	Descrição	Data
AWSDataLifecycleManagerAddedActionsToRoleForAMIManagement	O Amazon Data Lifecycle Manager adicionou as ações <code>ec2:EnableImageDeprecation</code> e <code>ec2:DisableImageDeprecation</code> para conceder permissão de políticas de AMI apoiadas pelo EBS para habilitar e desabilitar a defasagem da AMI.	20 de agosto de 2021
O Amazon Data Lifecycle Manager começou	O Amazon Data Lifecycle Manager começou a monitorar	23 de agosto de 2021

Alteração	Descrição	Data
a monitorar alterações	alterações para as políticas gerenciadas da AWS.	

Funções de serviço da IAM

Uma função AWS Identity and Access Management (IAM) é semelhante a um usuário do IAM, no sentido de ser uma identidade da AWS com políticas de permissão que determinam o que a identidade pode ou não fazer na AWS. No entanto, em vez de ser exclusivamente associada a uma pessoa, uma função destina-se a ser assumida por qualquer pessoa que precisar dela. Uma função de serviço é uma função que um serviço da AWS assume para realizar ações em seu nome. Como um serviço que executa as operações de backup para você, o Amazon Data Lifecycle Manager exige que você atribua uma função a ele ao executar operações de política para você. Para obter mais informações sobre funções do IAM, consulte [Funções do IAM](#) no Manual do usuário do IAM.

A função que você passa para o Amazon Data Lifecycle Manager deve ter uma política do IAM com as permissões que possibilitam que o Amazon Data Lifecycle Manager execute ações associadas a operações de política, como criar snapshots e AMIs, copiar snapshots e AMIs, excluir snapshots e cancelar o registro de AMIs. Diferentes permissões são necessárias para cada um dos tipos de política do Amazon Data Lifecycle Manager. A função também deve ter o Amazon Data Lifecycle Manager listado como uma entidade confiável, o que permite que o Amazon Data Lifecycle Manager assuma a função.

Tópicos

- [Funções de serviço padrão para o Amazon Data Lifecycle Manager \(p. 1397\)](#)
- [Funções de serviço personalizadas para o Amazon Data Lifecycle Manager \(p. 1398\)](#)

Funções de serviço padrão para o Amazon Data Lifecycle Manager

O Amazon Data Lifecycle Manager usa as seguintes funções de serviço padrão:

- `AWSDataLifecycleManagerDefaultRole`—função padrão para gerenciar snapshots. Ele confia apenas no serviço `dlm.amazonaws.com` para assumir a função e permite que o Amazon Data Lifecycle Manager execute as ações exigidas pelas políticas de cópia de snapshot e de snapshot entre contas em seu nome. Essa função usa a política gerenciada da `AWSDataLifecycleManagerServiceRole` AWS.
- `AWSDataLifecycleManagerDefaultRoleForAMIManagement`—função padrão para gerenciar AMIs. Ela confia apenas no serviço `dlm.amazonaws.com` para assumir a função e permite que o Amazon Data Lifecycle Manager execute as ações exigidas pelas políticas de AMI apoiadas pelo EBS para você. Essa função usa a política gerenciada da `AWSDataLifecycleManagerServiceRoleForAMIManagement` AWS.

Se você estiver usando o console do Amazon Data Lifecycle Manager, o Amazon Data Lifecycle Manager criará automaticamente a função de serviço `AWSDataLifecycleManagerDefaultRole` na primeira vez que você criar um snapshot ou política de cópia de snapshot entre contas e criará automaticamente a função de serviço `AWSDataLifecycleManagerDefaultRoleForAMIManagement` na primeira vez que você criar uma política de AMI baseada no EBS.

Se não estiver usando o console, você poderá criar as funções de serviço manualmente usando o comando `create-default-role`. Para `--resource-type`, especifique `snapshot` para criar `AWSDataLifecycleManagerDefaultRole` ou `image` para criar `AWSDataLifecycleManagerDefaultRoleForAMIManagement`.

```
$ aws dlm create-default-role --resource-type snapshot / image
```

Se você excluir essa função de serviço padrão e precisar criá-la novamente, poderá usar esse mesmo processo para recriar a função em sua conta.

Funções de serviço personalizadas para o Amazon Data Lifecycle Manager

Como alternativa ao uso das funções de serviço padrão, você pode criar funções do IAM personalizadas com as permissões necessárias e selecioná-las ao criar uma política de ciclo de vida.

Para criar uma função do IAM personalizada

1. Crie funções com as seguintes permissões.

- Permissões necessárias para gerenciar políticas de ciclo de vida de snapshot

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CreateSnapshot",  
                "ec2:CreateSnapshots",  
                "ec2>DeleteSnapshot",  
                "ec2:DescribeInstances",  
                "ec2:DescribeVolumes",  
                "ec2:DescribeSnapshots",  
                "ec2:EnableFastSnapshotRestores",  
                "ec2:DescribeFastSnapshotRestores",  
                "ec2:DisableFastSnapshotRestores",  
                "ec2:CopySnapshot",  
                "ec2:ModifySnapshotAttribute",  
                "ec2:DescribeSnapshotAttribute"  
            ],  
            "Resource": "*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2>CreateTags"  
            ],  
            "Resource": "arn:aws:ec2::::snapshot/*"  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "events:PutRule",  
                "events:DeleteRule",  
                "events:DescribeRule",  
                "events:EnableRule",  
                "events:DisableRule",  
                "events>ListTargetsByRule",  
                "events:PutTargets",  
                "events:RemoveTargets"  
            ],  
            "Resource": "arn:aws:events::::rule/AwsDataLifecycleRule.managed-cwe.*"  
        }  
    ]  
}
```

- Permissões necessárias para gerenciar políticas de ciclo de vida da AMI

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {
```

```
{  
    "Effect": "Allow",  
    "Action": "ec2:CreateTags",  
    "Resource": [  
        "arn:aws:ec2:::snapshot/*",  
        "arn:aws:ec2:::image/*"  
    ]  
,  
{  
    "Effect": "Allow",  
    "Action": [  
        "ec2:DescribeImages",  
        "ec2:DescribeInstances",  
        "ec2:DescribeImageAttribute",  
        "ec2:DescribeVolumes",  
        "ec2:DescribeSnapshots"  
    ],  
    "Resource": "*"  
,  
{  
    "Effect": "Allow",  
    "Action": "ec2>DeleteSnapshot",  
    "Resource": "arn:aws:ec2:::snapshot/*"  
,  
{  
    "Effect": "Allow",  
    "Action": [  
        "ec2:ResetImageAttribute",  
        "ec2:DeregisterImage",  
        "ec2>CreateImage",  
        "ec2:CopyImage",  
        "ec2:ModifyImageAttribute"  
    ],  
    "Resource": "*"  
}  
}
```

Para obter mais informações, consulte [Criar uma função](#) no Guia do usuário do IAM.

2. Adicione uma relação de confiança às funções.
 - a. No console do IAM, selecione Roles (Funções).
 - b. Selecione a função que você criou e, em seguida, escolha Relações de confiança.
 - c. Escolha Edit Trust Relationship (Editar relação de confiança), adicione a seguinte política e, em seguida, escolha Update Trust Policy (Atualizar política de confiança).

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Principal": {  
                "Service": "dlm.amazonaws.com"  
            },  
            "Action": "sts:AssumeRole"  
        }  
    ]  
}
```

Permissões para usuários do IAM

Um usuário do IAM deve ter as seguintes permissões para usar o Amazon Data Lifecycle Manager.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": ["iam:PassRole", "iam>ListRoles"],  
            "Resource": "arn:aws:iam::123456789012:role/AWSDataLifecycleManagerDefaultRole"  
        },  
        {  
            "Effect": "Allow",  
            "Action": "dlm:*",  
            "Resource": "*"  
        }  
    ]  
}
```

Para obter mais informações, consulte [Alteração de permissões para um usuário do IAM](#) no Guia do usuário do IAM.

Permissões para criptografia

Se o volume de origem for criptografado, verifique se as funções padrão do Amazon Data Lifecycle Manager, (AWSDataLifecycleManagerDefaultRole e AWSDataLifecycleManagerDefaultRoleForAMIManagement) têm permissão para usar as Chaves do KMS usadas para criptografar o volume.

Se você habilitar Cross Region copy (Cópia entre regiões) para snapshots não criptografados ou AMIs apoiadas por snapshots não criptografados e optar por ativar a criptografia na região de destino, verifique se as funções padrão têm permissão para usar a Chave do KMS necessária para executar a criptografia na região de destino.

Se você habilitar a Cross Region copy (Cópia entre regiões) para snapshots criptografados ou AMIs apoiadas por snapshots criptografados, verifique se as funções padrão têm permissão para usar as Chaves do KMS de origem e de destino.

Para obter mais informações, consulte [Allowing users in other accounts to use a KMS key](#) (Permitir que usuários de outras contas usem uma CMK) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

Monitorar o ciclo de vida de snapshots e AMIs

Você pode usar os seguintes recursos para monitorar o ciclo de vida de seus snapshots e AMIs.

Recursos

- [Console e AWS CLI \(p. 1400\)](#)
- [AWS CloudTrail \(p. 1401\)](#)
- [Monitorar políticas usando o CloudWatch Events \(p. 1401\)](#)
- [Monitorar políticas usando o Amazon CloudWatch \(p. 1402\)](#)

Console e AWS CLI

Você pode visualizar as políticas de ciclo de vida usando o console do Amazon EC2 ou a AWS CLI. Cada snapshot e AMI criada por uma política possui um timestamp e tags relacionadas à política. Você pode filtrar snapshots e AMIs usando tags para verificar se seus backups estão sendo criados conforme o esperado. Para obter informações sobre a visualização de políticas de ciclo de vida usando o console, consulte [Visualizar políticas de ciclo de vida \(p. 1391\)](#).

AWS CloudTrail

Com o AWS CloudTrail, você pode acompanhar as atividades do usuário e o uso da API para demonstrar a conformidade com as políticas internas e as normas reguladoras. Para obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

Monitorar políticas usando o CloudWatch Events

O Amazon EBS e o Amazon Data Lifecycle Manager geram eventos relacionados às ações das políticas de ciclo de vida. Você pode usar o AWS Lambda e o Amazon CloudWatch Events para tratar as notificações de eventos de forma programática. Eventos são emitidos com base no melhor esforço. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch Events](#).

Os seguintes eventos estão disponíveis:

Note

Nenhum evento é emitido para ações de política de ciclo de vida da AMI.

- `createSnapshot` – um evento do Amazon EBS gerado quando uma ação `CreateSnapshot` é bem-sucedida ou falha. Para obter mais informações, consulte [Amazon CloudWatch Events para Amazon EBS \(p. 1479\)](#).
- `DLM Policy State Change` – Um evento do Amazon Data Lifecycle Manager gerado quando uma política de ciclo de vida entra num estado de erro. O evento contém uma descrição do que causou o erro. O exemplo a seguir mostra um evento em que as permissões concedidas pela função do IAM não são suficientes.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-0123456789ab",  
    "detail-type": "DLM Policy State Change",  
    "source": "aws.dlm",  
    "account": "123456789012",  
    "time": "2018-05-25T13:12:22Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"  
    ],  
    "detail": {  
        "state": "ERROR",  
        "cause": "Role provided does not have sufficient permissions",  
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"  
    }  
}
```

O exemplo a seguir mostra um evento em que um limite é excedido.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-0123456789ab",  
    "detail-type": "DLM Policy State Change",  
    "source": "aws.dlm",  
    "account": "123456789012",  
    "time": "2018-05-25T13:12:22Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"  
    ],  
    "detail": {  
        "state": "ERROR",  
        "cause": "Maximum allowed active snapshot limit exceeded",  
    }  
}
```

```
        "policy_id": "arn:aws:dlm:us-east-1:123456789012:policy/policy-0123456789abcdef"
```

Monitorar políticas usando o Amazon CloudWatch

É possível monitorar as políticas de ciclo de vida do Amazon Data Lifecycle Manager usando o Amazon CloudWatch, que coleta e processa dados brutos em métricas legíveis quase que em tempo real. É possível usar essas métricas para ver exatamente quantos snapshots do Amazon EBS e AMIs baseadas no EBS são criados, excluídos e copiados por suas políticas ao longo do tempo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos.

As métricas ficam armazenadas por um período de 15 meses para que você possa acessar informações históricas e obter uma compreensão melhor sobre a performance de suas políticas de ciclo de vida em um período prolongado.

Para obter mais informações sobre o Amazon CloudWatch, consulte o [Guia do usuário do Amazon CloudWatch](#).

Tópicos

- [Métricas compatíveis \(p. 1402\)](#)
- [Visualizar métricas do CloudWatch para suas políticas \(p. 1405\)](#)
- [Métricas de gráfico para suas políticas \(p. 1406\)](#)
- [Criar um alarme do CloudWatch para uma política \(p. 1407\)](#)
- [Exemplo de casos de uso do \(p. 127\)](#)
- [Gerenciamento de políticas que relatam ações com falha \(p. 1409\)](#)

Métricas compatíveis

O namespace do Data Lifecycle Manager inclui as seguintes métricas das políticas de ciclo de vida do Amazon Data Lifecycle Manager. As métricas compatíveis diferem de acordo com o tipo de política.

Todas as métricas podem ser medidas na dimensão do `DLMPolicyId`. As estatísticas mais úteis são `sum` e `average`, e a unidade de medida é `count`.

Escolha uma guia para visualizar as métricas compatíveis com esse tipo de política.

EBS snapshot policies

Métrica	Descrição
<code>ResourcesTargeted</code>	O número de recursos de destino das tags especificadas em um snapshot ou política de AMI baseada no EBS.
<code>SnapshotsCreateStart</code>	O número de ações de criação de snapshots iniciadas por uma política de snapshot. Toda ação é registrada apenas uma vez, mesmo que haja várias tentativas subsequentes. Se uma ação de criação de snapshots falhar, o Amazon Data Lifecycle Manager enviará uma métrica <code>SnapshotsCreateFailed</code> .
<code>SnapshotsCreateCompleted</code>	O número de snapshots criados por uma política de snapshot. Inclui novas tentativas bem-sucedidas em até 60 minutos do horário agendado.

Métrica	Descrição
SnapshotsCreateFail	O número de snapshots que uma política de snapshot não conseguiu criar. Inclui novas tentativas malsucedidas em até 60 minutos do horário agendado.
SnapshotsSharedComp	O número de snapshots compartilhados entre contas por uma política de snapshot.
SnapshotsDeleteComp	O número de snapshots excluídos por um snapshot ou por uma política de AMI baseada no EBS. Essa métrica se aplica apenas aos snapshots criados pela política. Não se aplica a cópias de snapshots entre regiões criadas pela política. Essa métrica inclui snapshots que são excluídos quando uma política de AMI baseada no EBS cancela o registro de AMIs.
SnapshotsDeleteFail	O número de snapshots que o snapshot ou a política de AMI baseada no EBS não conseguiu excluir. Essa métrica se aplica apenas aos snapshots criados pela política. Não se aplica a cópias de snapshots entre regiões criadas pela política. Essa métrica inclui snapshots que são excluídos quando uma política de AMI baseada no EBS cancela o registro de AMIs.
SnapshotsCopiedRegion	O número de ações de cópia de snapshots entre regiões iniciadas por uma política de snapshot.
SnapshotsCopiedRegion	O número de ações de cópias de snapshots entre regiões criadas por uma política de snapshot. Inclui novas tentativas bem-sucedidas em até 24 horas do horário agendado.
SnapshotsCopiedRegion	O número de cópias de snapshots entre regiões que não foi possível criar por meio de uma política de snapshot. Inclui tentativas malsucedidas num prazo de 24 horas a partir do horário agendado.
SnapshotsCopiedRegion	O número de cópias de snapshots entre regiões excluídas, conforme designado pela regra de retenção, por uma política de snapshot.
SnapshotsCopiedRegion	O número de cópias de snapshots entre regiões que não foi possível excluir, conforme designado pela regra de retenção, por meio de uma política de snapshot.

EBS-backed AMI policies

As métricas a seguir podem ser usadas com políticas de AMI baseadas no EBS:

Métrica	Descrição
ResourcesTargeted	O número de recursos de destino das tags especificadas em um snapshot ou política de AMI baseada no EBS.
SnapshotsDeleteComp	O número de snapshots excluídos por um snapshot ou por uma política de AMI baseada no EBS. Essa métrica se aplica apenas aos snapshots criados pela política. Não se aplica a cópias de snapshots entre regiões criadas pela política.

Métrica	Descrição
	Essa métrica inclui snapshots que são excluídos quando uma política de AMI baseada no EBS cancela o registro de AMIs.
SnapshotsDeleteFailed	O número de snapshots que o snapshot ou a política de AMI baseada no EBS não conseguiu excluir. Essa métrica se aplica apenas aos snapshots criados pela política. Não se aplica a cópias de snapshots entre regiões criadas pela política.
	Essa métrica inclui snapshots que são excluídos quando uma política de AMI baseada no EBS cancela o registro de AMIs.
SnapshotsCopiedRegion	O número de cópias de snapshots entre regiões excluídas, conforme designado pela regra de retenção, por uma política de snapshot.
SnapshotsCopiedRegionFailed	O número de cópias de snapshots entre regiões que não foi possível excluir, conforme designado pela regra de retenção, por meio de uma política de snapshot.
ImagesCreateStarted	O número de ações CreateImage iniciadas por uma política de AMI baseada no EBS.
ImagesCreateCompleted	O número de AMIs criadas por uma política de AMI baseada no EBS.
ImagesCreateFailed	O número de AMIs que não foi possível criar por meio de uma política de AMI baseada pelo EBS.
ImagesDeregisterCompleted	O número de AMIs que tiveram o registro cancelado por uma política de AMI baseada no EBS.
ImagesDeregisterFailed	O número de AMIs cujo registro não foi possível cancelar por meio de uma política de AMI baseada no EBS.
ImagesCopiedRegionStarted	O número de ações de cópia entre regiões iniciadas por uma política de AMI baseada no EBS.
ImagesCopiedRegionCompleted	O número de cópias de AMIs entre regiões criadas por uma política de AMI baseada no EBS.
ImagesCopiedRegionFailed	O número de cópias de AMIs entre regiões que não foi possível criar por meio de uma política de AMI baseada no EBS.
ImagesCopiedRegionDeleted	O número de cópias de AMIs entre regiões que tiveram o registro cancelado, conforme designado pela regra de retenção, por meio de uma política de AMI baseada no EBS.
ImagesCopiedRegionDeletedFailed	O número de cópias de AMIs entre regiões cujo registro não foi possível cancelar, conforme designado pela regra de retenção, por meio de uma política de AMI baseada no EBS.
EnableImageDeprecationCompleted	O número de AMIs que foram marcadas para defasagem por meio de uma política de AMI baseada no EBS.
EnableImageDeprecationFailed	O número de AMIs que não puderam ser marcadas para defasagem por meio de uma política de AMI baseada no EBS.
EnableCopiedImageDeprecationCompleted	O número de cópias AMI entre Regiões que foram marcadas para defasagem por meio de uma política de AMI baseada no EBS.

Métrica	Descrição
EnableCopiedImageDeployment	Quantidade de cópias AMI entre Regiões que não puderam ser marcadas para defasagem por meio de uma política de AMI baseada no EBS.

Cross-account copy event policies

As seguintes métricas podem ser usadas com políticas de eventos de cópia entre contas:

Métrica	Descrição
SnapshotsCopiedAccount	Quantidade de ações de cópia de snapshots entre contas iniciadas por uma política de eventos de cópia entre contas.
SnapshotsCopiedAccount	Quantidade de snapshots copiados de outra conta por uma política de eventos de cópia entre contas. Inclui novas tentativas bem-sucedidas em até 24 horas do horário agendado.
SnapshotsCopiedAccount	Quantidade de snapshots que não foi possível copiar de outra conta por meio de uma política de eventos de cópia entre contas. Inclui tentativas malsucedidas num prazo de 24 horas do horário agendado.
SnapshotsCopiedAccount	Quantidade de cópias de snapshots entre regiões excluídas, conforme designado pela regra de retenção, por uma política de evento de cópia entre contas.
SnapshotsCopiedAccount	Quantidade de cópias de snapshots entre regiões que não foi possível excluir, conforme designado pela regra de retenção, por meio de uma política de evento de cópia entre contas.

Visualizar métricas do CloudWatch para suas políticas

Você pode usar o AWS Management Console ou as ferramentas da linha de comando para listar as métricas que o Amazon Data Lifecycle Manager envia ao Amazon CloudWatch.

Amazon EC2 console

Para visualizar as métricas usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Gerenciador de ciclo de vida.
3. Selecione uma política na grade e, em seguida, escolha a guia Monitoramento.

CloudWatch console

Para visualizar as métricas usando o console do Amazon CloudWatch

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. No painel de navegação, selecione Metrics (Métricas).
3. Selecione o namespace do EBS e selecione as métricas do Data Lifecycle Manager.

AWS CLI

Para listar todas as métricas disponíveis para o Amazon Data Lifecycle Manager

Use o comando [list-metrics](#).

```
C:\> aws cloudwatch list-metrics --namespace AWS/EBS
```

Para listar todas as métricas para uma política específica

Use o comando [list-metrics](#) e especifique a dimensão `DLMPolicyId`.

```
C:\> aws cloudwatch list-metrics --namespace AWS/EBS --dimensions  
Name=DLMPolicyId,Value=policy-abcdef01234567890
```

Para listar uma métrica única em todas as políticas

Use o comando [list-metrics](#) e especifique a opção `--metric-name`.

```
C:\> aws cloudwatch list-metrics --namespace AWS/EBS --metric-  
name SnapshotsCreateCompleted
```

Métricas de gráfico para suas políticas

Depois que criar uma política, você pode abrir o console do Amazon EC2 e ver os gráficos de monitoramento para a instância na guia Monitoramento. Cada gráfico se baseia em uma das métricas disponíveis do Amazon EC2.

As métricas de gráficos a seguir estão disponíveis:

- Recursos direcionados (com base em `ResourcesTargeted`)
- Criação de snapshots iniciada (com base em `SnapshotsCreateStarted`)
- Criação de snapshots concluída (com base em `SnapshotsCreateCompleted`)
- Falha na criação de snapshots (com base em `SnapshotsCreateFailed`)
- Compartilhamento de snapshots concluído (com base em `SnapshotsSharedCompleted`)
- Exclusão de snapshot concluída (com base em `SnapshotsDeleteCompleted`)
- Falha na exclusão de snapshots (com base em `SnapshotsDeleteFailed`)
- Cópia de snapshots entre Regiões iniciada (com base em `SnapshotsCopiedRegionStarted`)
- Cópia de snapshots entre Regiões concluída (com base em `SnapshotsCopiedRegionCompleted`)
- Falha na cópia de snapshots entre Regiões (com base em `SnapshotsCopiedRegionFailed`)
- Exclusão da cópia de snapshots entre Regiões concluída (com base em `SnapshotsCopiedRegionDeleteCompleted`)
- Falha na exclusão da cópia de snapshots entre Regiões (com base em `SnapshotsCopiedRegionDeleteFailed`)
- Cópia de snapshots entre contas iniciada (com base em `SnapshotsCopiedAccountStarted`)
- Cópia de snapshots entre contas concluída (com base em `SnapshotsCopiedAccountCompleted`)
- Falha na cópia de snapshots entre contas (com base em `SnapshotsCopiedAccountFailed`)
- Exclusão da cópia de snapshots entre contas concluída (com base em `SnapshotsCopiedAccountDeleteCompleted`)
- Falha na exclusão da cópia de snapshots entre contas (com base em `SnapshotsCopiedAccountDeleteFailed`)
- Criação de AMI iniciada (com base em `ImagesCreateStarted`)
- Criação de AMI concluída (com base em `ImagesCreateCompleted`)
- Falha na criação de AMI (com base em `ImagesCreateFailed`)

- Cancelamento de registro de AMI concluído (com base em `ImagesDeregisterCompleted`)
- Falha no cancelamento do registro da AMI (com base em `ImagesDeregisterFailed`)
- Cópia de AMI entre Regiões iniciada (com base em `ImagesCopiedRegionStarted`)
- Cópia de AMI entre Regiões concluída (com base em `ImagesCopiedRegionCompleted`)
- Falha na cópia de AMI entre Regiões (com base em `ImagesCopiedRegionFailed`)
- Cancelamento de registro de cópia de AMI entre Regiões concluída (com base em `ImagesCopiedRegionDeregisterCompleted`)
- Falha no cancelamento de registro da cópia de AMI entre Regiões (com base em `ImagesCopiedRegionDeregisteredFailed`)
- AMI para habilitar defasagem concluído (com base em `EnableImageDeprecationCompleted`)
- Falha na AMI para habilitar defasagem (com base em `EnableImageDeprecationFailed`)
- Cópia da AMI para habilitar defasagem entre Regiões concluída (com base em `EnableCopiedImageDeprecationCompleted`)
- Falha na cópia da AMI para habilitar defasagem entre Regiões (com base em `EnableCopiedImageDeprecationFailed`)

Criar um alarme do CloudWatch para uma política

É possível criar um alarme do CloudWatch que monitore métricas do CloudWatch para as suas políticas. O CloudWatch lhe enviará automaticamente uma notificação quando a métrica atingir um limite que você especificou. É possível criar um alarme do CloudWatch usando o console do CloudWatch.

Para obter informações sobre como criar alarmes usando o console do CloudWatch, consulte o Manual do usuário do Amazon CloudWatch.

- [Criar um alarme do CloudWatch com base em um limite estático](#)
- [Criar um alarme do CloudWatch com base na detecção de anomalias](#)

Exemplo de casos de uso do

Veja a seguir exemplos de casos de uso:

Tópicos

- [Exemplo 1: métrica ResourcesTargeted \(p. 1407\)](#)
- [Exemplo 2: métrica SnapshotDeleteFailed \(p. 1408\)](#)
- [Exemplo 3: métrica SnapshotsCopiedRegionFailed \(p. 1408\)](#)

Exemplo 1: métrica ResourcesTargeted

É possível usar a métrica `ResourcesTargeted` para monitorar o número total de recursos de destino de uma política específica toda vez que ela é executada. Isso permite acionar um alarme quando o número de recursos de destino estiver abaixo ou acima do limite esperado.

Por exemplo, se você espera que sua política diária crie backups de não mais do que 50 volumes, é possível criar um alarme que envia uma notificação por e-mail quando a `sum` de `ResourcesTargeted` for maior que 50 pelo período de 1 hora. Dessa forma, é possível garantir que nenhum snapshot tenha sido criado inesperadamente de volumes que foram etiquetados de maneira incorreta.

Você pode usar o seguinte comando para criar este alarme:

```
C:\> aws cloudwatch put-metric-alarm \
--alarm-name resource-targeted-monitor \
--alarm-description "Alarm when policy targets more than 50 resources" \
```

```
--metric-name ResourcesTargeted \
--namespace AWS/EBS \
--statistic Sum \
--period 3600 \
--threshold 50 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=DLMPolicyId,Value=policy_id" \
--evaluation-periods 1 \
--alarm-actions sns_topic_arn
```

Exemplo 2: métrica SnapshotDeleteFailed

Você pode usar a métrica `SnapshotDeleteFailed` para monitorar falhas na exclusão de snapshots, conforme a regra de retenção de snapshots da política.

Por exemplo, se você tiver criado uma política que deve excluir snapshots automaticamente a cada 12 horas, será possível criar um alarme que notifique sua equipe de engenharia quando a `sum` de `SnapshotDeletionFailed` for maior que 0 pelo período de 1 hora. Isso pode ajudar a averiguar a retenção incorreta de snapshots e a garantir que os custos de armazenamento não aumentem por causa de snapshots desnecessários.

Você pode usar o seguinte comando para criar este alarme:

```
C:\> aws cloudwatch put-metric-alarm \
--alarm-name snapshot-deletion-failed-monitor \
--alarm-description "Alarm when snapshot deletions fail" \
--metric-name SnapshotsDeleteFailed \
--namespace AWS/EBS \
--statistic Sum \
--period 3600 \
--threshold 0 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=DLMPolicyId,Value=policy_id" \
--evaluation-periods 1 \
--alarm-actions sns_topic_arn
```

Exemplo 3: métrica SnapshotsCopiedRegionFailed

Use a métrica `SnapshotsCopiedRegionFailed` para identificar quando suas políticas apresentam falha ao copiar snapshots para outras regiões.

Por exemplo, se sua política copia snapshots entre regiões diariamente, é possível criar um alarme que envia um SMS para sua equipe de engenharia quando a `sum` de `SnapshotCrossRegionCopyFailed` for maior que 0 pelo período de 1 hora. Isso pode ser útil para verificar se a política copiou corretamente os snapshots subsequentes na linhagem.

Você pode usar o seguinte comando para criar este alarme:

```
C:\> aws cloudwatch put-metric-alarm \
--alarm-name snapshot-copy-region-failed-monitor \
--alarm-description "Alarm when snapshot copy fails" \
--metric-name SnapshotsCopiedRegionFailed \
--namespace AWS/EBS \
--statistic Sum \
--period 3600 \
--threshold 0 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=DLMPolicyId,Value=policy_id" \
--evaluation-periods 1 \
--alarm-actions sns_topic_arn
```

Gerenciamento de políticas que relatam ações com falha

Para obter mais informações sobre o que fazer quando uma de suas políticas relatar um valor inesperado diferente de zero para uma métrica de ação com falha, consulte a seção [O que devo fazer se o Amazon Data Lifecycle Manager relatar ações com falha nas métricas do CloudWatch? AWS](#).

Serviços de dados do Amazon EBS

O Amazon EBS fornece os seguintes serviços de dados.

Serviços de dados

- [Volumes elásticos do Amazon EBS \(p. 1409\)](#)
- [Criptografia de Amazon EBS \(p. 1422\)](#)
- [Restauração rápida de snapshots do Amazon EBS \(p. 1434\)](#)

Volumes elásticos do Amazon EBS

É possível aumentar o tamanho dos volumes elásticos do Amazon EBS, alterar o tipo de volume ou ajustar a performance de seus volumes do EBS. Se a sua instância oferecer suporte aos Elastic Volumes, você poderá fazê-lo sem desanexar o volume ou reiniciar a instância. Isso permite que você continue usando sua aplicação enquanto as alterações entram em vigor.

Não há cobrança para modificar a configuração de um volume. Você será cobrado pela configuração de novo volume após o início da modificação do volume. Para obter mais informações, consulte a página de [Definição de preço do Amazon EBS](#).

Tópicos

- [Requisitos ao modificar volumes \(p. 1409\)](#)
- [Solicitar modificações para seus volumes do EBS \(p. 1411\)](#)
- [Monitorar o progresso das modificações de volume \(p. 1414\)](#)
- [Estender um sistema de arquivos Windows após um redimensionamento do volume \(p. 1417\)](#)

Requisitos ao modificar volumes

Os seguintes requisitos e limitações se aplicam quando você modifica um volume do Amazon EBS. Para saber mais sobre os requisitos gerais para volumes do EBS, consulte [Restrições de tamanho e configuração de um volume do EBS \(p. 1265\)](#).

Tópicos

- [Tipos de instâncias compatíveis \(p. 1409\)](#)
- [Requisitos para volumes do Windows \(p. 1410\)](#)
- [Limitations \(p. 1410\)](#)

Tipos de instâncias compatíveis

Elastic Volumes são compatíveis com as seguintes instâncias:

- [Todas as instâncias da geração atual \(p. 149\)](#)
- As seguintes instâncias de geração anterior: C1, C3, CC2, CR1, G2, I2, M1, M3 e R3

Se o tipo de instância não oferecer suporte a Elastic Volumes, consulte [Modificar um volume do EBS se não houver suporte para Elastic Volumes \(p. 1414\)](#).

Requisitos para volumes do Windows

Por padrão, o Windows inicializa volumes com uma tabela de partição do registro mestre de inicialização (MBR). Como o MBR é compatível apenas com volumes menores que 2 TiB (2.048 GiB), o Windows impede você de redimensionar volumes MBR para além desse limite. Nesse caso, a opção Extend Volume (Estender volume) é desabilitada no utilitário Disk Management (Gerenciamento de disco) do Windows. Se você usa o AWS Management Console ou a AWS CLI para criar um volume particionado como MBR que excede o limite de tamanho, o Windows não pode detectar ou usar o espaço adicional. Para requisitos que afetam os volumes do Linux, consulte [Requisitos para volumes do Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Para superar esse limite, você pode criar um novo volume maior com uma tabela de partição de GUID (GPT) e copiar sobre os dados a partir do volume MBR original.

Para criar um volume GPT

1. Crie um novo volume vazio do tamanho desejado na zona de disponibilidade da instância do EC2 e anexe-o à sua instância.

Note

O novo volume não deve estar em um volume restaurado de um snapshot.

2. Faça login em seu sistema Windows e abra o Gerenciamento de disco (diskmgmt.exe).
3. Abra o menu de contexto (clique com o botão direito do mouse) do novo disco e escolha Online.
4. Na janela Inicializar disco, selecione o novo disco e escolha GPT (tabela de partição GUID), OK.
5. Quando a inicialização estiver concluída, copie os dados do volume original para o novo volume usando uma ferramenta como robocopy ou teracopy.
6. Em Gerenciamento de disco, altere as letras das unidades para os valores apropriados e coloque o antigo volume no modo offline.
7. No console do Amazon EC2, desanexe o volume da instância, reinicie a instância para verificar se ela funciona corretamente, e exclua o antigo volume.

Limitations

- Há limites para o armazenamento agregado máximo que pode ser solicitado em todas as modificações de volume. Para obter mais informações, consulte [Cotas de serviço do Amazon EBS](#) no Amazon Web Services General Reference.
- Depois de modificar um volume, é necessário aguardar pelo menos seis horas e garantir que o volume esteja no estado `in-use` ou `available` para poder modificar o mesmo volume. Às vezes isso é referenciado como período de desaquecimento.
- Se o volume foi anexado antes de 3 de novembro de 2016, às 23h40 UTC, é necessário inicializar o suporte aos Elastic Volumes. Para obter mais informações, consulte [Como inicializar o suporte aos Elastic Volumes \(p. 1413\)](#).
- Se você encontrar uma mensagem de erro ao tentar modificar em um volume do EBS, ou se estiver modificando um volume do EBS associado a um tipo de instância da geração anterior, obtenha uma das seguintes etapas:
 - Para um volume não raiz, separe o volume da instância, aplique as modificações e reassocie o volume.
 - Para um volume do dispositivo raiz, interrompa a instância, aplique as modificações e reinicie a instância.
- O tempo de modificação é aumentado para volumes que não estão totalmente inicializados. Para obter mais informações, consulte [Iniciar volumes do Amazon EBS \(p. 1463\)](#).
- O novo tamanho do volume não pode exceder a capacidade compatível de seu sistema de arquivos e esquema de particionamento. Para obter mais informações, consulte [Restrições de tamanho e configuração de um volume do EBS \(p. 1265\)](#).

- Se você modificar o tipo de volume de um volume, o tamanho e a performance devem estar dentro dos limites do tipo de volume de destino. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#)
- Não é possível diminuir o tamanho de um volume do EBS. No entanto, você pode criar um volume menor e migrar seus dados para ele usando uma ferramenta em nível de aplicação, como robocopy.
- Depois de provisionar mais de 32.000 IOPS em um volume io1 ou io2 existente, talvez seja necessário desvincular e reanexar o volume ou reiniciar a instância para ver todos os aprimoramentos de performance.
- Para volumes io2, não é possível aumentar seu tamanho além de 16 TiB ou suas IOPS além de 64,000 enquanto o volume está anexado a um tipo de instância que não é compatível com volumes io2 do Block Express. No momento, somente instâncias R5b oferecem suporte a volumes io2 do Block Express. Para obter mais informações, consulte [Volumes io2 do Block Express \(p. 1256\)](#)
- Não é possível modificar o tamanho ou as IOPS provisionadas de um volume io2 anexado a uma instância R5B.
- Não é possível modificar o tipo de volume de volumes io2 habilitados por Multi-Attach.
- Não é possível modificar o tipo, o tamanho ou as IOPS provisionadas de volumes io1 habilitados para Multi-Attach.
- Um volume do gp2 anexado a uma instância como um volume raiz não poderá ser modificado para um volume do st1 ou sc1. Se desvinculado e modificado para st1 ou sc1, não poderá ser reanexado a uma instância como o volume raiz.
- Embora as instâncias m3.medium sejam totalmente compatíveis com a modificação de volume, as instâncias m3.large, m3.xlarge e m3.2xlarge podem não ser compatíveis com todos os recursos da modificação de volume.

Solicitar modificações para seus volumes do EBS

Com os Elastic Volumes, é possível aumentar dinamicamente o tamanho, a performance e o tipo de volume dos volumes do Amazon EBS sem desvinculá-los.

Use o seguinte processo ao modificar um volume:

1. (Opcional) Antes de modificar um volume que contém dados valiosos, a prática recomendada é criar um snapshot de volume caso você precise voltar suas alterações. Para obter mais informações, consulte [Criar snapshots de Amazon EBS \(p. 1298\)](#).
2. Solicite a modificação do volume.
3. Monitore o progresso da modificação do volume. Para obter mais informações, consulte [Monitorar o progresso das modificações de volume \(p. 1414\)](#).
4. Se o tamanho do volume tiver sido alterado, estenda o sistema de arquivos de volume para aproveitar o aumento da capacidade de armazenamento. Para obter mais informações, consulte [Estender um sistema de arquivos Windows após um redimensionamento do volume \(p. 1417\)](#).

Tópicos

- [Modificar um volume do EBS usando volumes elásticos \(p. 1411\)](#)
- [Iniciar o suporte aos Elastic Volumes \(se necessário\) \(p. 1413\)](#)
- [Modificar um volume do EBS se não houver suporte para Elastic Volumes \(p. 1414\)](#)

Modificar um volume do EBS usando volumes elásticos

Só é possível aumentar o tamanho do volume. É possível aumentar ou diminuir a performance do volume. Se você não estiver alterando o tipo de volume, as modificações no tamanho e na performance do volume

devem estar dentro dos limites do tipo de volume atual. Se você não estiver alterando o tipo de volume, as modificações no tamanho e na performance do volume devem estar dentro dos limites do tipo de volume de destino.

Para modificar um volume do EBS, use um dos métodos a seguir.

Console

Para modificar um volume EBS usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Selecione Volumes, selecione o volume a ser modificado e escolha Actions, Modify Volume.
3. A janela Modify Volume (Modificar volume) exibe o ID de volume e a configuração atual do volume, incluindo tipo, tamanho, IOPS e taxa de transferência. Defina os novos valores de configuração da forma a seguir:
 - Para modificar o tipo, escolha um valor para Tipo de volume.
 - Para modificar o tamanho, insira um novo valor para Size (Tamanho).
 - Para modificar as IOPS, se o tipo de volume for gp3io1, ou io2, insira um novo valor para IOPS.
 - Para modificar a taxa de transferência, se o tipo de volume for gp3, insira um novo valor para Throughput (Taxa de transferência).
4. Após a alteração das configurações de volume, selecione Modify (Modificar). Quando a confirmação for solicitada, selecione Yes (Sim).
5. Modificar o tamanho do volume não tem nenhum efeito prático até você também estender o sistema de arquivos do volume para usar a nova capacidade de armazenamento. Para obter mais informações, consulte [Estender um sistema de arquivos Windows após um redimensionamento do volume \(p. 1417\)](#).
6. Se você aumentar o tamanho de um volume NVMe em uma instância que não tem os drivers do AWS NVMe, você deve reiniciar a instância para permitir que o Windows visualize o novo tamanho do volume. Para obter mais informações sobre a instalação dos drivers do AWS NVMe, consulte [AWSDrivers NVMe para instâncias do Windows \(p. 580\)](#).

AWS CLI

Para modificar um volume EBS usando a AWS CLI

Use o comando `modify-volume` para modificar uma ou mais definições de configuração de um volume. Por exemplo, se você tiver um volume do tipo gp2 com um tamanho de 100 GiB, o comando a seguir alterará a configuração para um volume do tipo io1 com 10.000 IOPS e um tamanho de 200 GiB.

```
aws ec2 modify-volume --volume-type io1 --iops 10000 --size 200 --volume-id vol-1111111111111111
```

A seguir está um exemplo de saída:

```
{  
    "VolumeModification": {  
        "TargetSize": 200,  
        "TargetVolumeType": "io1",  
        "ModificationState": "modifying",  
        "VolumeId": "vol-1111111111111111",  
        "TargetIops": 10000,  
        "StartTime": "2017-01-19T22:21:02.959Z",  
        "Progress": 0,  
        "Status": "in-progress"  
    }  
}
```

```
        "OriginalVolumeType": "gp2",
        "OriginalIops": 300,
        "OriginalSize": 100
    }
}
```

Modificar o tamanho do volume não tem nenhum efeito prático até você também estender o sistema de arquivos do volume para usar a nova capacidade de armazenamento. Para obter mais informações, consulte [Estender um sistema de arquivos Windows após um redimensionamento do volume \(p. 1417\)](#).

[Iniciar o suporte aos Elastic Volumes \(se necessário\)](#)

Antes de ser possível modificar um volume que foi anexado a uma instância antes de 3 de novembro de 2016, às 23h40 UTC, é necessário inicializar o suporte à modificação de volumes usando uma das seguintes ações:

- Desanexar e anexar o volume
- Interromper e iniciar a instância

Use um dos procedimentos a seguir para determinar se suas instâncias estão prontas para modificação de volume.

New console

Para determinar se suas instâncias estão prontas usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione o ícone Show/Hide Columns (a engrenagem). Selecione a coluna de atributos Launch time (Tempo de execução) e escolha Confirm (Confirmar).
4. Classifique a lista de instâncias pela coluna Launch Time. Para cada instância iniciada antes da data limite, escolha a guia Storage (Armazenamento) e verifique a coluna Attachment time (Hora da associação) para ver quando os volumes foram anexados.

Old console

Para determinar se suas instâncias estão prontas usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione o ícone Show/Hide Columns (a engrenagem). Selecione os atributos Launch Time e Block Devices e escolha Close.
4. Classifique a lista de instâncias pela coluna Launch Time. Para instâncias que foram iniciadas antes da data de interrupção, verifique quando os dispositivos foram anexados. No exemplo a seguir, é necessário inicializar a modificação de volume para a primeira instância porque ela foi iniciada antes da data de interrupção e o volume de raiz dela foi anexado antes da data de interrupção. As outras instâncias estão prontas porque foram iniciadas após a data de interrupção.

Instance ID	Launch Time	Block Devices
i-e905622e	February 25, 2016 at 1:49:35 PM UTC-8	/dev/xvda=vol-e6b6d6410 attached:2016-02-25T21:49:35.000Z:true
i-719f99a8	December 8, 2016 at 2:21:51 PM UTC-8	/dev/xvda=vol-bad60e7a attached:2016-01-15T18:36:12.000Z:true
i-006b02c1b78381e57	May 17, 2017 at 1:52:52 PM UTC-7	/dev/sda1=vol-0de9250441c73024c:attached:2017-05-17T20:52:53.000Z:true, xvdb=vol-0863a86c393496d3d:attached:2017-05-17T20:52:53.000Z:false
i-e3d172ed	May 17, 2017 at 2:48:54 PM UTC-7	/dev/sda1=vol-04c34d0b:attached:2015-01-21T21:19:46.000Z:true

AWS CLI

Para determinar se suas instâncias estão prontas usando a CLI

Use o comando [describe-instances](#) a seguir para determinar se o volume foi anexado antes de 3 de novembro de 2016, às 23h40 UTC.

```
aws ec2 describe-instances --query "Reservations[*].Instances[*].  
[InstanceId,LaunchTime<='2016-11-01',BlockDeviceMappings[*]  
[Ebs.AttachTime<='2016-11-01']]" --output text
```

A primeira linha da saída de cada instância mostra o ID dela e se foi iniciada antes da data de interrupção (True ou False). A primeira linha é seguida por uma ou mais linhas que mostram se cada volume do EBS foi anexado antes da data de interrupção (True ou False). No exemplo de saída a seguir, é necessário inicializar a modificação de volume para a primeira instância porque ela foi iniciada antes da data de interrupção e o volume de raiz dela foi anexado antes da data de interrupção. As outras instâncias estão prontas porque foram iniciadas após a data de interrupção.

```
i-e905622e      True  
True  
i-719f99a8      False  
True  
i-006b02c1b78381e57  False  
False  
False  
i-e3d172ed      False  
True
```

Modificar um volume do EBS se não houver suporte para Elastic Volumes

Se estiver usando um tipo de instância com suporte, você poderá utilizar Elastic Volumes para modificar dinamicamente o tamanho, a performance e o tipo de volume dos seus volumes do Amazon EBS sem desanexá-los.

Se não puder usar Elastic Volumes, mas precisar modificar o volume raiz (inicialização), você deverá parar a instância, modificar o volume e reiniciar a instância.

Após a instância ter sido iniciada, você pode verificar o tamanho do sistema de arquivos para ver se sua instância reconhece o espaço de volume maior.

Se o tamanho não refletir o volume recém-expandido, amplie o sistema de arquivos do seu dispositivo para que a instância possa usar o novo espaço. Para obter mais informações, consulte [Estender um sistema de arquivos Windows após um redimensionamento do volume \(p. 1417\)](#).

Você pode ter de colocar o volume online para usá-lo. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#). Você não precisa reformatar o volume.

Monitorar o progresso das modificações de volume

Quando você modifica um volume do EBS, ele atravessa uma sequência de estados. O volume insere o estado `modifying`, o estado `optimizing` e, por fim, o estado `completed`. Neste ponto, o volume está pronto para ser modificado ainda mais.

Note

Raramente, uma falha temporária da AWS pode resultar em um estado `failed`. Isso não é uma indicação da integridade do volume. Apenas indica que houve falha na modificação do volume. Se isso ocorrer, tente novamente a modificação do volume.

Quando o volume está no estado `optimizing`, sua performance de volume está entre as especificações de configuração de origem e de destino. A performance de volume transitório não será menor que a

performance de volume de origem. Se você está fazendo downgrade do IOPS, a performance do volume transitório não é inferior à performance do volume de destino.

As alterações de modificação de volume entram em vigor da seguinte forma:

- Alterações de tamanho geralmente demoram alguns segundos para serem concluídas e entram em vigor depois que o volume mudar para o estado Optimizing.
- As alterações de performance (IOPS) pode levar de alguns minutos a algumas horas para serem concluídas e dependem das alterações de configuração que estão sendo feitas.
- Pode demorar até 24 horas para uma nova configuração entrar em vigor e, em alguns outros casos mais, como quando o volume não tiver sido totalmente inicializado. Normalmente, um volume de 1 TiB totalmente usado demora cerca de 6 horas para migrar uma nova configuração de performance.

Use um dos métodos a seguir para monitorar o progresso de uma modificação de volume.

Amazon EC2 console

Para monitorar o progresso de uma modificação usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes.
3. Selecione o volume.
4. A coluna State (Estado) e o campo State (Estado) no painel de detalhes contêm informações no seguinte formato: volume-state - modification-state (progress%). Os possíveis estados de volume são creating (criando), available (disponível), in use (em uso), deleting (excluindo), deleted (excluído) e error (com erro). Os possíveis estados de modificação são modifying (modificando), optimizing (otimizando) e completed (concluído). Logo após a conclusão da modificação do volume, removemos o estado e o andamento da modificação, deixando apenas o estado do volume.

Neste exemplo, o estado de modificação do volume selecionado é optimizing (otimizando). O estado da modificação do próximo volume é modifying (modificando).

The screenshot shows the Amazon EC2 console interface. At the top, there is a table titled "Volumes" with columns: Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, and State. One row is selected, showing a volume with Volume ID "vol-02940f6ee433f..." and State "in-use - optimizing (1%)". Below the table, there are tabs for Description, Status Checks, Monitoring, and Tags. The "Description" tab is active, displaying detailed information about the selected volume. This includes fields like Volume ID, Size, Created, State, Attachment information (with an ID "i-00142a" highlighted), Volume type (gp2), Product codes, and IOPS (100). To the right of these details, there is a "Volume modification details" section which is currently empty. Further down, there are sections for Alarm status (None), Snapshot (snap-076d641...), Availability Zone (eu-west-1c), Encryption (Not Encrypted), KMS Key ID, KMS Key Aliases, KMS Key ARN, and Multi-Attach Enabled (No).

5. Escolha o texto no campo State (Estado) no painel de detalhes para exibir informações sobre a ação de modificação mais recente, conforme mostrado na etapa anterior.

AWS CLI

Para monitorar o progresso de uma modificação usando a AWS CLI

Use o comando [describe-volumes-modifications](#) para visualizar o progresso de uma ou mais modificações de volume. O exemplo a seguir descreve as modificações de volume para dois volumes.

```
aws ec2 describe-volumes-modifications --volume-  
ids vol-1111111111111111 vol-2222222222222222
```

Na saída de exemplo a seguir, as modificações de volume ainda estão no estado `modifying`. O andamento é relatado como uma porcentagem.

```
{  
    "VolumesModifications": [  
        {  
            "TargetSize": 200,  
            "TargetVolumeType": "io1",  
            "ModificationState": "modifying",  
            "VolumeId": "vol-1111111111111111",  
            "TargetIops": 10000,  
            "StartTime": "2017-01-19T22:21:02.959Z",  
            "Progress": 0,  
            "OriginalVolumeType": "gp2",  
            "OriginalIops": 300,  
            "OriginalSize": 100  
        },  
        {  
            "TargetSize": 2000,  
            "TargetVolumeType": "sc1",  
            "ModificationState": "modifying",  
            "VolumeId": "vol-2222222222222222",  
            "StartTime": "2017-01-19T22:23:22.158Z",  
            "Progress": 0,  
            "OriginalVolumeType": "gp2",  
            "OriginalIops": 300,  
            "OriginalSize": 1000  
        }  
    ]  
}
```

O exemplo a seguir descreve todos os volumes com um estado de modificação `optimizing` ou `completed` e filtra e formata os resultados para mostrar somente as modificações iniciadas em ou depois de 1º de fevereiro de 2017:

```
aws ec2 describe-volumes-modifications --filters Name=modification-  
state,Values="optimizing","completed" --query "VolumesModifications[?  
StartTime>='2017-02-01'].{ID:VolumeId,STATE:ModificationState}"
```

A seguir, um exemplo de saída com informações sobre dois volumes:

```
[  
    {  
        "STATE": "optimizing",  
        "ID": "vol-06397e7a0eEXAMPLE"  
    },  
    {  
        "STATE": "completed",  
        "ID": "vol-ba74e18c2aEXAMPLE"  
    }  
]
```

CloudWatch Events console

Com o CloudWatch Events, você pode criar uma regra de notificação para eventos de modificação de volume. Você pode usar a regra para gerar uma mensagem de notificação usando o [Amazon SNS](#) ou invocar uma [função do Lambda](#) em resposta a eventos correspondentes. Eventos são emitidos com base no melhor esforço.

Para monitorar o progresso de uma modificação usando o CloudWatch Events

1. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
2. Escolha Eventos, Criar regra.
3. Para Construir padrão de eventos para corresponder a eventos por serviço, escolha Padrão de eventos personalizado.
4. Para Build custom event pattern (Construir padrão de eventos personalizado), substitua o conteúdo pelo seguinte e escolha Save (Salvar).

```
{  
    "source": [  
        "aws.ec2"  
    ],  
    "detail-type": [  
        "EBS Volume Notification"  
    ],  
    "detail": {  
        "event": [  
            "modifyVolume"  
        ]  
    }  
}
```

Veja a seguir um exemplo de dados de evento:

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Volume Notification",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "2017-01-12T21:09:07Z",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"  
    ],  
    "detail": {  
        "result": "optimizing",  
        "cause": "",  
        "event": "modifyVolume",  
        "request-id": "01234567-0123-0123-0123-0123456789ab"  
    }  
}
```

Estender um sistema de arquivos Windows após um redimensionamento do volume

Depois de aumentar o tamanho de um volume do EBS, use o utilitário de gerenciamento de disco do Windows ou o PowerShell para expandir o tamanho do disco até o novo tamanho do volume. Você pode começar a redimensionar o sistema de arquivos à medida que o volume entrar no estado **optimizing**.

Para obter mais informações sobre esse utilitário, consulte [Estender um volume básico](#) no site do Microsoft Docs.

Para obter mais informações sobre como estender um sistema de arquivos no Linux, consulte [Como estender um sistema de arquivos Linux após um redimensionamento do volume](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

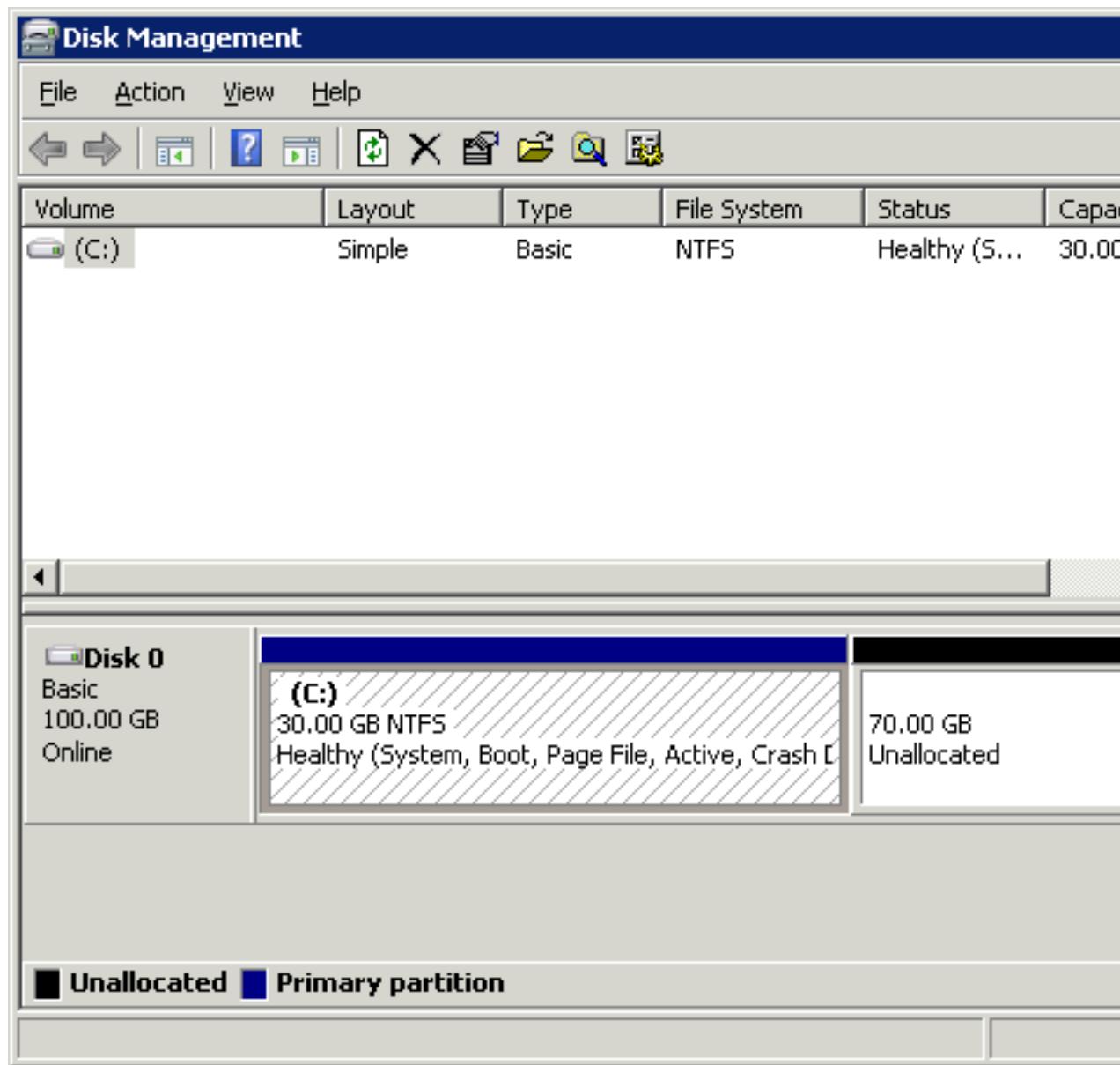
- [Estender um sistema de arquivos Windows usando o utilitário de gerenciamento de disco \(p. 1418\)](#)
- [Estender um sistema de arquivos Windows usando o PowerShell \(p. 1421\)](#)

[Estender um sistema de arquivos Windows usando o utilitário de gerenciamento de disco](#)

Use o procedimento a seguir para estender um sistema de arquivos do Windows usando o Gerenciamento de disco.

[Como estender um sistema de arquivos usando o Gerenciamento de disco](#)

1. Antes de estender um sistema de arquivos que contém dados valiosos, o melhor é criar um snapshot do volume que o contém, caso você precise voltar suas alterações. Para obter mais informações, consulte [Criar snapshots de Amazon EBS \(p. 1298\)](#).
2. Execute a sessão da sua instância do Windows usando o Desktop Remoto.
3. Na caixa de diálogo Run (Executar), digite diskmgmt.msc e pressione Enter. O utilitário de gerenciamento de disco se abre.

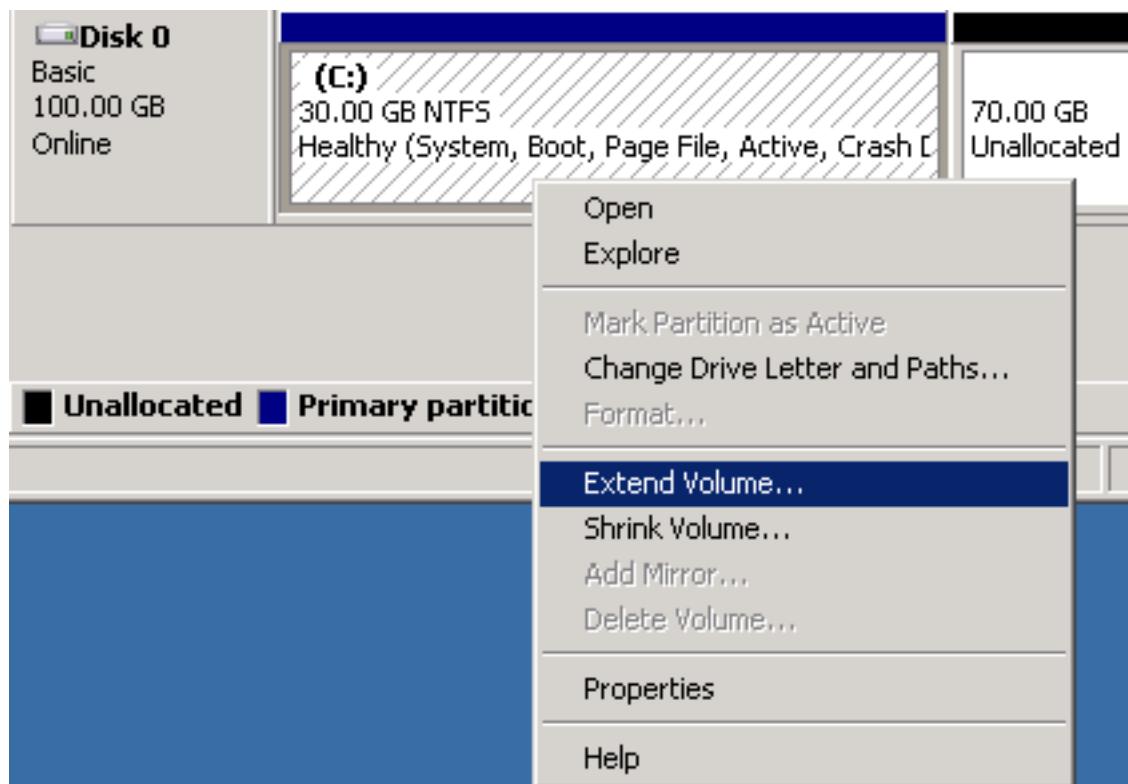


4. No menu Gerenciamento de Disco, escolha Ação, Examinar Discos Novamente.
5. Abra o menu contextual (botão direito do mouse) da unidade expandida e escolha Estender volume.

Note

Extend Volume (Estender volume) pode ser desativado (acinzentado) se:

- O espaço não alocado não é adjacente ao drive. O espaço não alocado deve ser adjacente ao lado direito da unidade que você deseja estender.
- O volume usa o estilo de partição Master Boot Record (MBR) e já tem 2 TB. Os volumes que usam MBR não podem exceder 2 TB.



6. No assistente Extend Volume (Estender volume), selecione Next (Próximo). Para Selecionar o espaço em MB, digite o número de megabytes pelos quais ampliar o volume. Geralmente, você especifica o espaço máximo disponível. O texto destacado em Selected é a quantidade de espaço que será adicionada, não o tamanho final que o volume terá. Assista todo o assistente.

Extend Volume Wizard

Select Disks

You can use space on one or more disks to extend the volume.

You can only extend the volume to the available space shown below because your disk cannot be converted to dynamic or the volume being extended is a boot or system volume.

Available:

Add >

< Remove

< Remove All

Selected:

Disk 0	71679 MB
--------	----------

Total volume size in megabytes (MB):

102397

Maximum available space in MB:

71679

Select the amount of space in MB:

71679



< Back

Next >

Cancel

7. Se você aumentar o tamanho de um volume NVMe em uma instância que não tem o driver do AWS NVMe, você deve reiniciar a instância para permitir que o Windows visualize o novo tamanho do volume. Para obter mais informações sobre a instalação do driver do AWS NVMe, consulte [AWS Drivers NVMe para instâncias do Windows \(p. 580\)](#).

Estender um sistema de arquivos Windows usando o PowerShell

Use o procedimento a seguir para estender um sistema de arquivos do Windows usando o PowerShell.

Como estender um sistema de arquivos usando o PowerShell

1. Antes de estender um sistema de arquivos que contém dados valiosos, o melhor é criar um snapshot do volume que o contém, caso você precise voltar suas alterações. Para obter mais informações, consulte [Criar snapshots de Amazon EBS \(p. 1298\)](#).
2. Execute a sessão da sua instância do Windows usando o Desktop Remoto.
3. Execute o PowerShell como administrador.
4. Execute o comando `Get-Partition`. O PowerShell retornará o número da partição correspondente, a mensagem da unidade, o deslocamento, o tamanho e o tipo. Observe a letra da unidade da partição a ser estendida.

- Execute o seguinte comando para verificar o disco novamente.

```
"rescan" | diskpart
```

- Execute o seguinte comando, usando a mensagem da unidade que você anotou na etapa 4 no lugar de <drive-letter>. O PowerShell retornará o tamanho mínimo e máximo da partição permitida, em bytes.

```
Get-PartitionSupportedSize -DriveLetter <drive-letter>
```

- Para estender a partição, execute o comando a seguir, inserindo o novo tamanho do volume no lugar de <size>. É possível inserir o tamanho em KB, MB e GB, por exemplo, 24GB.

```
Resize-Partition -DriveLetter <drive-letter> -Size <size>
```

Veja a seguir o fluxo completo de comando e resposta para estender um sistema de arquivos usando o PowerShell.

```
PS C:\Users\Administrator> Get-Partition

Disk Number: 0

PartitionNumber DriveLetter Offset
----- -----
1                  1048576
2                  C          368050176
                                         Size Type
                                         ----- -----
                                         350 MB IFS
                                         29.66 GB IFS

Disk Number: 1

PartitionNumber DriveLetter Offset
----- -----
1                  D          1048576
                                         Size Type
                                         ----- -----
                                         6 GB IFS

PS C:\Users\Administrator> "rescan" | diskpart

Microsoft DiskPart version 6.3.9600

Copyright (C) 1999-2013 Microsoft Corporation.

On computer:

DISKPART>
Please wait while DiskPart scans your configuration...

DiskPart has finished scanning your configuration.

DISKPART> PS C:\Users\Administrator> Get-PartitionSupportedSize -DriveLetter C

                                         SizeMin
                                         -----
                                         23356313600

PS C:\Users\Administrator> Resize-Partition -DriveLetter C -Size 24GB
PS C:\Users\Administrator> _
```

Criptografia de Amazon EBS

Use Criptografia de Amazon EBS como solução de criptografia direta para seus recursos do EBS associados às instâncias do EC2. Com a criptografia do Amazon EBS, não é necessário criar, manter e

proteger sua própria infraestrutura de gerenciamento de chaves. A criptografia do Amazon EBS usa AWS KMS keys ao criar volumes e snapshots criptografados.

As operações de criptografia ocorrem nos servidores que hospedam instâncias do EC2, garantindo a segurança dos dados em repouso e dos dados em trânsito entre uma instância e seu armazenamento do EBS anexado.

Você pode anexar volumes criptografados e não criptografados a uma instância simultaneamente.

Tópicos

- [Como funciona a criptografia do EBS \(p. 1423\)](#)
- [Requirements \(p. 1424\)](#)
- [Padrão Chave do KMS para criptografia EBS \(p. 1425\)](#)
- [Criptografia por padrão \(p. 1426\)](#)
- [Criptografar recursos do EBS \(p. 1427\)](#)
- [Cenários de criptografia \(p. 1428\)](#)
- [Configurar padrões de criptografia usando a API e a CLI \(p. 1434\)](#)

Como funciona a criptografia do EBS

É possível criptografar os volumes de dados e inicialização de uma instância do EC2.

Quando você cria um volume do EBS criptografado e o anexa a um tipo de instância com suporte, os seguintes tipos de dados são criptografados:

- Dados em repouso dentro do volume
- Todos os dados que são movidos entre o volume e a instância
- Todos os snapshots criados a partir do volume
- Todos os volumes criados a partir desses snapshots

O EBS criptografa o volume com uma chave de dados usando o algoritmo AES-256 padrão do setor. A chave de dados é armazenada em disco com seus dados criptografados, mas não antes que o EBS a criptografe com a Chave do KMS. A chave de dados nunca é exibida no disco em texto simples. A mesma chave de dados é compartilhada pelos snapshots do volume e de quaisquer volumes subsequentes criados a partir desses snapshots. Para obter mais informações, consulte [Data keys \(Chaves de dados\)](#) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

O Amazon EC2 trabalha com o AWS KMS para criptografar e descriptografar os volumes do EBS de maneiras ligeiramente diferentes, ou seja, dependendo se o snapshot a partir do qual você cria um volume criptografado é criptografado ou não criptografado.

Como funciona a criptografia EBS quando o snapshot é criptografado

Quando você cria um volume criptografado a partir de um snapshot criptografado que você possui, o Amazon EC2 trabalha com o AWS KMS para criptografar e descriptografar os volumes do EBS da seguinte forma:

1. O Amazon EC2 envia uma solicitação [GenerateDataKeyWithoutPlaintext](#) ao AWS KMS especificando a chave do KMS que você escolheu para a criptografia de volume.
2. O AWS KMS gera uma nova chave de dados, criptografa-a com a chave do KMS escolhida para a criptografia de volume e envia a chave de dados criptografada ao Amazon EBS para ser armazenada com os metadados do volume.
3. Quando você anexa o volume criptografado a uma instância, o Amazon EC2 envia uma solicitação [CreateGrant](#) ao AWS KMS para que ele possa descriptografar a chave de dados.

4. O AWS KMS descriptografa a chave de dados criptografada e envia a chave de dados descriptografada ao Amazon EC2.
5. O Amazon EC2 usa a chave de dados de texto simples na memória do hipervisor para criptografar a E/S de disco para o volume. A chave de dados de texto simples persistirá na memória enquanto o volume estiver anexado à instância.

Como funciona a criptografia EBS quando o snapshot não é criptografado

Quando você cria um volume criptografado a partir de um snapshot não criptografado, o Amazon EC2 trabalha com o AWS KMS para criptografar e descriptografar os volumes do EBS da seguinte forma:

1. O Amazon EC2 envia uma solicitação [CreateGrant](#) ao AWS KMS para que ele possa criptografar o volume criado a partir do snapshot.
2. O Amazon EC2 envia uma solicitação [GenerateDataKeyWithoutPlaintext](#) ao AWS KMS especificando a chave do KMS que você escolheu para a criptografia de volume.
3. O AWS KMS gera uma nova chave de dados, criptografa-a com a chave do KMS escolhida para a criptografia de volume e envia a chave de dados criptografada ao Amazon EBS para ser armazenada com os metadados do volume.
4. O Amazon EC2 envia uma solicitação [Decrypt](#) ao AWS KMS para obter a chave de criptografia para criptografar os dados de volume.
5. Quando você anexa o volume criptografado a uma instância, o Amazon EC2 envia uma solicitação [CreateGrant](#) ao AWS KMS para que ele possa descriptografar a chave de dados.
6. Quando você anexa um volume criptografado a uma instância, o Amazon EC2 envia uma solicitação [Decrypt](#) ao AWS KMS especificando a chave de dados criptografada.
7. O AWS KMS descriptografa a chave de dados criptografada e envia a chave de dados descriptografada ao Amazon EC2.
8. O Amazon EC2 usa a chave de dados de texto simples na memória do hipervisor para criptografar a E/S de disco para o volume. A chave de dados de texto simples persistirá na memória enquanto o volume estiver anexado à instância.

Para obter mais informações, consulte [How Amazon Elastic Block Store \(Amazon EBS\) uses AWS KMS](#) (Como o Amazon Elastic Block Store (Amazon EBS) usa o AWS KMS) e [Amazon EC2 example two](#) (Exemplo dois do Amazon EC2) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do Amazon Key Management Service).

Requirements

Antes de começar, verifique se os seguintes requisitos foram atendidos.

Tipos de volume compatíveis

A criptografia é compatível com todos os tipos de volume do EBS. Você pode esperar a mesma performance de IOPS dos volumes não criptografados nos volumes criptografados, com efeito mínimo na latência. Você pode acessar volumes criptografados da mesma forma que acessa volumes não criptografados. A criptografia e a descriptografia são tratadas de forma transparente e não requerem nenhuma ação adicional de sua parte e de suas aplicações.

Tipos de instâncias compatíveis

Criptografia de Amazon EBS está disponível em todos os tipos de instância da [geração atual \(p. 150\)](#) e nos seguintes tipos de instância da [geração anterior \(p. 152\)](#): A1, C3, cr1.8xlarge, G2, I2, M3, and R3.

Permissões para usuários do IAM

Quando você configura uma Chave do KMS como a chave padrão para a criptografia do EBS, a política de Chave do KMS padrão permite que qualquer usuário do IAM com acesso às ações necessárias do KMS

use essa Chave do KMS para criptografar ou descriptografar os recursos do EBS. Você deve conceder aos usuários do IAM a permissão para chamar as seguintes ações para usar a criptografia do EBS:

- kms:CreateGrant
- kms:Decrypt
- kms:DescribeKey
- kms:GenerateDataKeyWithoutPlainText
- kms:ReEncrypt

Para seguir o princípio de menor privilégio, não permita acesso total a kms:CreateGrant. Em vez disso, permita que o usuário crie concessões na chave do KMS somente quando a concessão for criada em nome do usuário por um produto da AWS conforme mostrado no exemplo a seguir.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": "kms>CreateGrant",  
            "Resource": [  
                "arn:aws:kms:us-east-2:123456789012:key/abcd1234-a123-456d-a12b-  
a123b4cd56ef"  
            ],  
            "Condition": {  
                "Bool": {  
                    "kms:GrantIsForAWSResource": true  
                }  
            }  
        }  
    ]  
}
```

Para obter mais informações, consulte [Allows access to the AWS account and enables IAM policies](#) (Permite acesso à conta da AWS e ativa políticas do IAM) na seção Default key policy (Política de chaves padrão) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

Padrão Chave do KMS para criptografia EBS

O Amazon EBS cria automaticamente uma Chave gerenciada pela AWS exclusiva em cada região em que você armazena recursos da AWS. Essa Chave do KMS tem o alias alias/aws/ebs. Por padrão, o Amazon EBS usa essa Chave do KMS para a criptografia. Como alternativa, você pode especificar uma simétrica chave gerenciada pelo cliente criada como padrão Chave do KMS para a criptografia EBS. Usar sua própria Chave do KMS oferece a você mais flexibilidade, incluindo a capacidade de criar, alternar e desabilitar Chaves do KMS.

Important

O Amazon EBS não oferece suporte a Chaves do KMS assimétricas. Para obter mais informações, consulte [Using symmetric and asymmetric keys](#) (Usar chaves simétricas e assimétricas) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

New console

Como configurar a Chave do KMS padrão para a criptografia do EBS em uma região

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. Na barra de navegação, selecione a região.
3. No painel de navegação, selecione EC2 Dashboard (Painel do EC2).
4. No canto superior direito da página, escolha Account Attributes (Atributos da conta), EBS encryption (Criptografia do EBS).
5. Escolha Gerenciar.
6. Para a Chave de criptografia padrão, escolha uma chave gerenciada pelo cliente simétrica.
7. Escolha Update EBS encryption (Atualizar criptografia do EBS).

Old console

Como configurar a Chave do KMS padrão para a criptografia do EBS em uma região

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região.
3. No painel de navegação, selecione EC2 Dashboard (Painel do EC2).
4. No canto superior direito da página, escolha Account Attributes (Atributos da conta), Settings (Configurações).
5. Escolha Change the default key (Alterar a chave padrão) e selecione uma Chave do KMS disponível.
6. Escolha Save settings (Salvar configurações).

Criptografia por padrão

Você poderá configurar sua conta da AWS para impor a criptografia das novas cópias de snapshots e volumes do EBS que criar. Por exemplo, o Amazon EBS criptografará os volumes do EBS criados quando você executar uma instância e os snapshots que copiar a partir de um snapshot não criptografado. Para obter exemplos da transição de recursos do EBS não criptografados para criptografados, consulte [Criptografar recursos não criptografados \(p. 1428\)](#).

Por padrão, a criptografia não tem efeito sobre volumes ou snapshots do EBS existentes.

Considerações

- A criptografia por padrão é uma configuração específica da região. Se você habilitá-la para uma região, não será possível desabilitá-la para snapshots ou volumes individuais nessa região.
- Ao habilitar a criptografia por padrão, você poderá executar uma instância somente se o tipo de instância oferecer suporte à criptografia do EBS. Para obter mais informações, consulte [Tipos de instâncias compatíveis \(p. 1424\)](#).
- Se você copiar um snapshot e criptografá-lo com uma nova chave do KMS, será criada uma cópia completa (não incremental). Isso resulta em custos adicionais de armazenamento.
- Ao migrar servidores usando o AWS Server Migration Service (SMS), não ative a criptografia por padrão. Se a criptografia por padrão já estiver ativada, e você estiver enfrentando falhas de replicação delta, desative a criptografia por padrão. Em vez disso, habilite a criptografia de AMI ao criar o trabalho de replicação.

New console

Para ativar a criptografia por padrão para uma região

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. Na barra de navegação, selecione a região.
3. No painel de navegação, selecione EC2 Dashboard (Painel do EC2).
4. No canto superior direito da página, escolha Account Attributes (Atributos da conta), EBS encryption (Criptografia do EBS).
5. Escolha Gerenciar.
6. Selecione Enable (Habilitar). Mantenha a Chave gerenciada pela AWS com o alias `alias/aws/ebs` criado em seu nome como a chave de criptografia padrão ou escolha uma chave simétrica gerenciada pelo cliente.
7. Escolha Update EBS encryption (Atualizar criptografia do EBS).

Old console

Para ativar a criptografia por padrão para uma região

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a região.
3. No painel de navegação, selecione EC2 Dashboard (Painel do EC2).
4. No canto superior direito da página, escolha Account Attributes (Atributos da conta), Settings (Configurações).
5. Em EBS Storage (Armazenamento do EBS), selecione Always encrypt new EBS volumes (Sempre criptografar novos volumes do EBS).
6. Escolha Save settings (Salvar configurações).

Não é possível alterar a Chave do KMS que está associada a um snapshot existente ou a um volume criptografado. No entanto, você pode associar uma Chave do KMS diferente durante uma operação de cópia de snapshot para que o snapshot copiado resultante seja criptografado pela nova Chave do KMS.

Criptografar recursos do EBS

Criptografe volumes do EBS habilitando a criptografia, usando a [criptografia por padrão \(p. 1426\)](#) ou habilitando a criptografia ao criar um volume que deseja criptografar.

Ao criptografar um volume, você pode especificar a Chave do KMS simétrica a ser usada para criptografar o volume. Se a Chave do KMS não for especificada, a Chave do KMS usada para a criptografia dependerá do estado de criptografia do snapshot de origem e de sua propriedade. Para obter mais informações, consulte a [tabela de resultados de criptografia \(p. 1432\)](#).

Note

Se você estiver usando a API ou a AWS CLI para especificar uma chave do KMS, esteja ciente de que a AWS autentica Chave do KMS de forma assíncrona. Se você especificar um ID de Chave do KMS, um alias ou um ARN que não forem válidos, é possível que a ação pareça estar concluída, mas ela falhará eventualmente.

Você não pode alterar a Chave do KMS que estiver associada a um snapshot ou a um volume existente. No entanto, você pode associar uma Chave do KMS diferente durante uma operação de cópia de snapshot para que o snapshot copiado resultante seja criptografado pela nova Chave do KMS.

Criptografar um volume vazio na criação

Ao criar um novo volume do EBS vazio, você poderá criptografá-lo habilitando a criptografia para a operação de criação de volume específica. Se você tiver habilitado a criptografia do EBS por padrão, o volume será automaticamente criptografado usando a Chave do KMS padrão para criptografia do EBS.

Outra opção é especificar uma Chave do KMS simétrica diferente para a operação de criação de um volume específico. O volume será criptografado no momento em que for disponibilizado a primeira vez, para que seus dados estejam sempre protegidos. Para ver os procedimentos detalhados, consulte [Crie um volume do Amazon EBS.](#) (p. 1268).

Por padrão, a Chave do KMS selecionada durante a criação de um volume criptografa os snapshots que você cria do volume e os volumes que você restaura desses snapshots criptografados. Não é possível remover a criptografia de um volume ou snapshot criptografado, o que significa que um volume restaurado a partir de um snapshot criptografado ou uma cópia de um snapshot criptografado será sempre criptografado.

Não há suporte para snapshots públicos de volumes criptografado, mas você pode compartilhar um snapshot criptografado com contas específicas. Para obter instruções detalhadas, consulte [Compartilhar um snapshot do Amazon EBS](#) (p. 1323).

Criptografar recursos não criptografados

Não é possível criptografar diretamente volumes ou snapshots não criptografados. No entanto, você pode criar volumes ou snapshots criptografados a partir de volumes ou snapshots não criptografados. Se você habilitar a criptografia por padrão, o Amazon EBS automaticamente criptografa o novo volume ou snapshot usando a chave KMS padrão para a criptografia do EBS. Caso contrário, você poderá habilitar a criptografia ao criar um volume ou um snapshot individual, usando a Chave KMS padrão para a criptografia do EBS ou uma chave simétrica gerenciada pelo cliente. Para obter mais informações, consulte [Crie um volume do Amazon EBS.](#) (p. 1268) e [Copiar um snapshot do Amazon EBS.](#) (p. 1317).

Para criptografar a cópia do snapshot para uma chave gerenciada pelo cliente, você deve habilitar a criptografia e especificar a Chave do KMS, conforme mostrado em [Copiar um snapshot não criptografado \(criptografia por padrão não habilitada\)](#) (p. 1430).

Important

O Amazon EBS não oferece suporte a Chaves do KMS assimétricas. Para obter mais informações, consulte [Using symmetric and asymmetric keys](#) (Usar chaves simétricas e assimétricas) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

Também é possível aplicar novos estados de criptografia ao executar uma instância a partir de uma AMI baseada em EBS. Isso ocorre porque as AMIs baseadas em EBS incluem snapshots de volumes do EBS que podem ser criptografados conforme descrito. Para obter mais informações, consulte [Usar criptografia com AMIs com EBS](#) (p. 135).

Cenários de criptografia

Quando você cria um recurso do EBS criptografado, ele é criptografado pela Chave do KMS padrão para a criptografia do EBS da sua conta, a menos que você especifique uma chave gerenciada pelo cliente diferente nos parâmetros de criação do volume ou no mapeamento de dispositivos de blocos para a AMI ou para a instância. Para obter mais informações, consulte [Padrão Chave do KMS para criptografia EBS](#) (p. 1425).

Os exemplos a seguir ilustram como você pode gerenciar o estado de criptografia de seus volumes e snapshots. Para obter uma lista completa de casos de criptografia, consulte a [tabela de resultados de criptografia](#) (p. 1432).

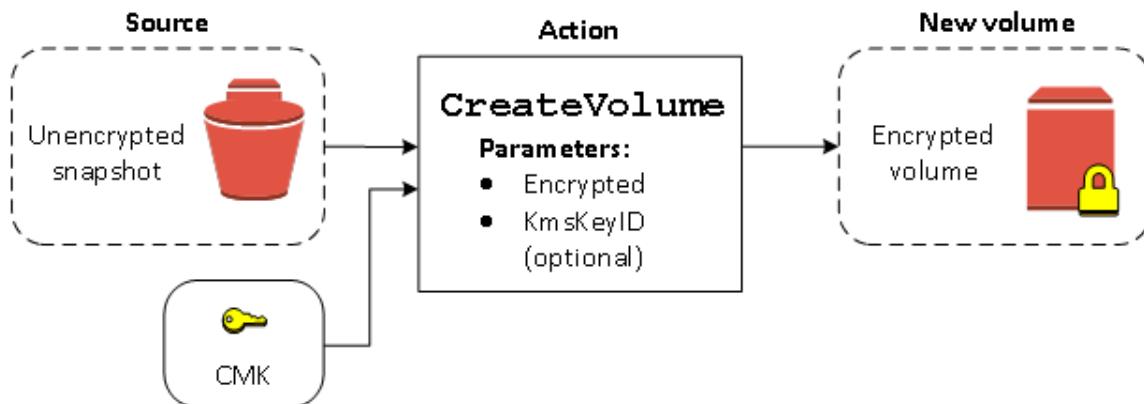
Exemplos

- [Restaurar um volume não criptografado \(criptografia por padrão não habilitada\)](#) (p. 1429)
- [Restaurar um volume não criptografado \(criptografia por padrão habilitada\)](#) (p. 1429)
- [Copiar um snapshot não criptografado \(criptografia por padrão não habilitada\)](#) (p. 1430)

- Copiar um snapshot não criptografado (criptografia por padrão habilitada) (p. 1430)
- Criptografar novamente um volume criptografado (p. 1430)
- Criptografar novamente um snapshot criptografado (p. 1431)
- Migrar dados entre volumes criptografados e não criptografados (p. 1431)
- Resultados da criptografia (p. 1432)

Restaurar um volume não criptografado (criptografia por padrão não habilitada)

Sem a criptografia por padrão habilitada, um volume restaurado de um snapshot não criptografado é não criptografado por padrão. No entanto, é possível criptografar o volume resultante configurando o parâmetro `Encrypted` e, opcionalmente, o parâmetro `KmsKeyId`. O diagrama a seguir ilustra o processo.

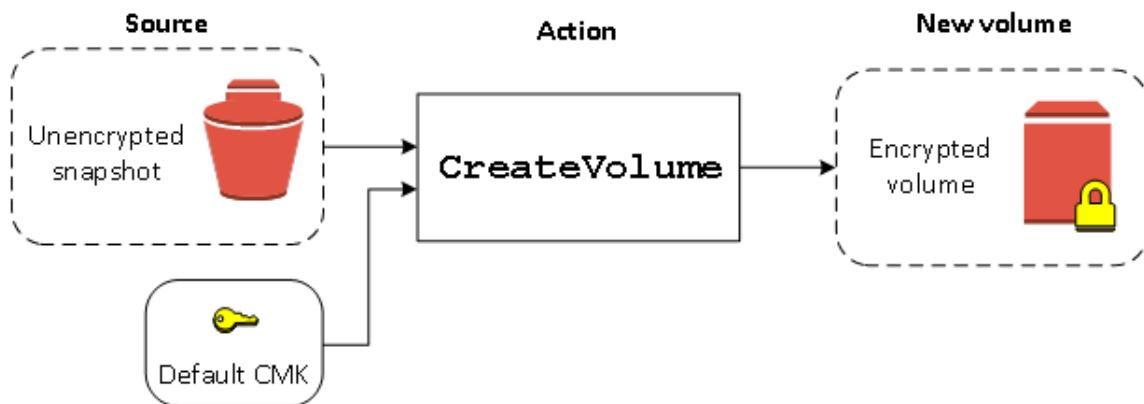


Se você deixar o parâmetro `KmsKeyId` de fora, o volume resultante será criptografado usando a Chave do KMS padrão para a criptografia do EBS. Você deve especificar o ID de uma Chave do KMS para criptografar o volume de uma Chave do KMS diferente.

Para obter mais informações, consulte [Criar um volume a partir de um snapshot \(p. 1270\)](#).

Restaurar um volume não criptografado (criptografia por padrão habilitada)

Quando a criptografia for habilitada por padrão, ela será obrigatória para volumes restaurados de snapshots não criptografados, e nenhum parâmetro de criptografia será necessário para que a Chave do KMS padrão seja usada. O diagrama a seguir mostra este simples caso padrão:

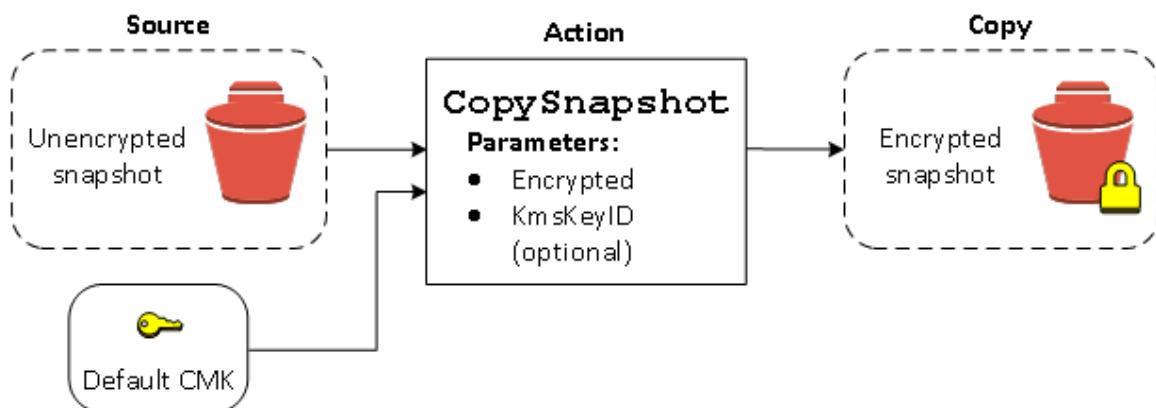


Se quiser criptografar o volume restaurado para uma `Encrypted` simétrica, você deverá fornecer os parâmetros chave gerenciada pelo cliente e `KmsKeyId`, conforme mostrado em [Restaurar um volume não criptografado \(criptografia por padrão não habilitada\) \(p. 1429\)](#).

Copiar um snapshot não criptografado (criptografia por padrão não habilitada)

Sem a criptografia por padrão habilitada, uma cópia de um snapshot não criptografado é não criptografado por padrão. No entanto, é possível criptografar o snapshot resultante configurando o parâmetro `Encrypted` e, opcionalmente, o parâmetro `KmsKeyId`. Se você omitir o `KmsKeyId`, o snapshot resultante será criptografado pela Chave do KMS padrão. É necessário especificar o ID de uma Chave do KMS para criptografar o volume para uma Chave do KMS simétrica diferente.

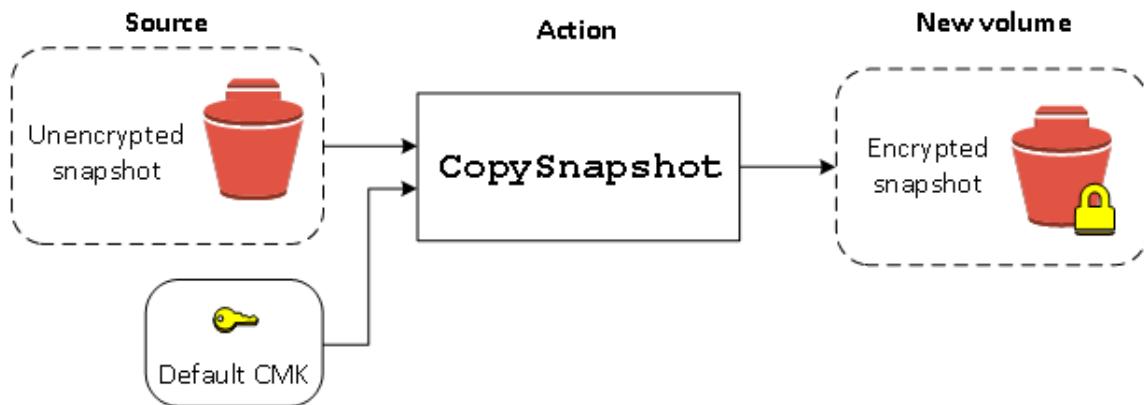
O diagrama a seguir ilustra o processo.



Você pode criptografar um volume do EBS ao copiar um snapshot não criptografado em um snapshot criptografado e criar um volume a partir do snapshot criptografado. Para obter mais informações, consulte [Copiar um snapshot do Amazon EBS. \(p. 1317\)](#).

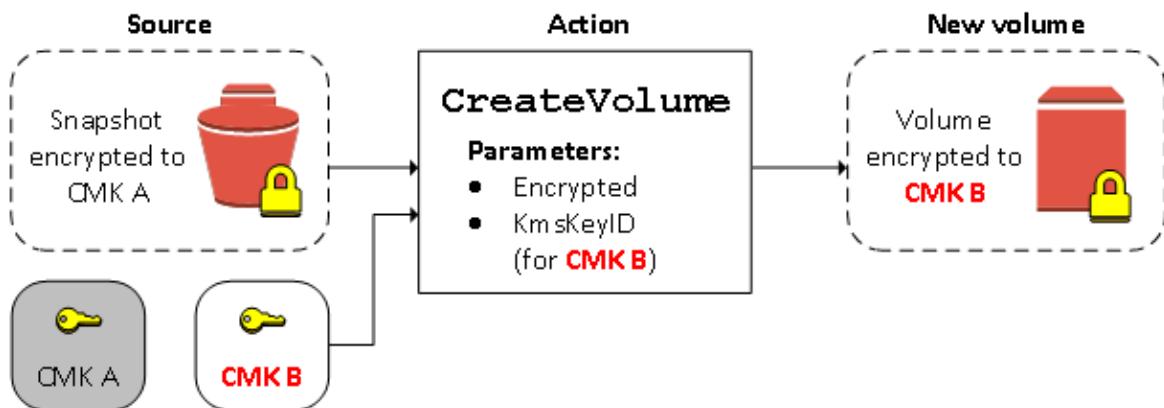
Copiar um snapshot não criptografado (criptografia por padrão habilitada)

Quando a criptografia por padrão estiver habilitada, a criptografia é obrigatória para cópias de snapshots não criptografados, e nenhum parâmetro de criptografia será necessário se a Chave do KMS padrão for usada. O diagrama a seguir ilustra este caso padrão:



Criptografar novamente um volume criptografado

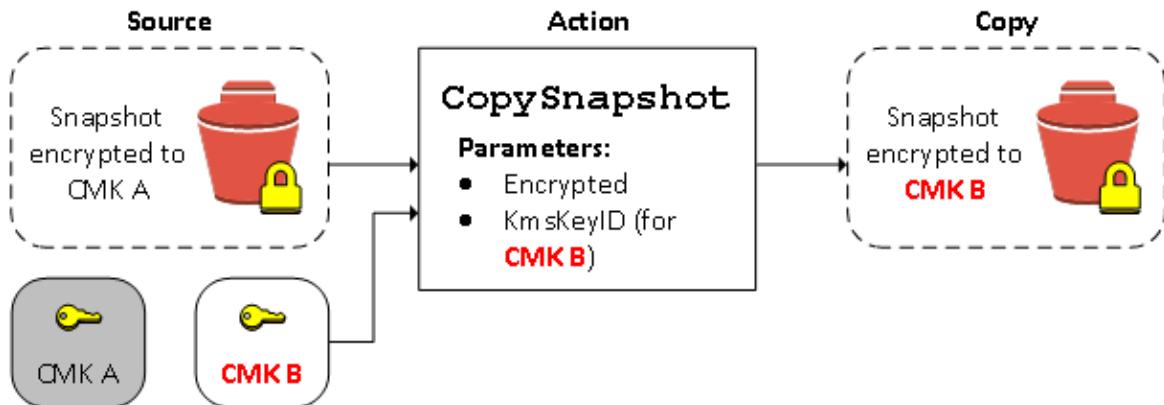
Quando a ação `CreateVolume` opera em um snapshot criptografado, você tem a opção de criptografá-lo novamente com uma Chave do KMS diferente. O diagrama a seguir ilustra o processo. Neste exemplo, você tem duas Chaves do KMS: Chave do KMS A e Chave do KMS B. O snapshot de origem é criptografado pela Chave do KMS A. Durante a criação do volume, com o ID de Chave do KMS da Chave do KMS B especificado como um parâmetro, os dados de origem são automaticamente descriptografados e, depois, novamente criptografados pela Chave do KMS B.



Para obter mais informações, consulte [Criar um volume a partir de um snapshot \(p. 1270\)](#).

Criptografar novamente um snapshot criptografado

A capacidade de criptografar um snapshot durante a cópia permite aplicar uma nova Chave do KMS simétrica a um snapshot já criptografado de sua propriedade. Os volumes restaurados da cópia resultante só são acessíveis usando a nova Chave do KMS. O diagrama a seguir ilustra o processo. Neste exemplo, você tem duas Chaves do KMS: Chave do KMS A e Chave do KMS B. O snapshot de origem é criptografado pela Chave do KMS A. Durante a cópia, com o ID de Chave do KMS da Chave do KMS B especificado como um parâmetro, os dados de origem são novamente criptografados de forma automática pela Chave do KMS B.



Em um cenário relacionado, você pode optar por aplicar novos parâmetros de criptografia a uma cópia de um snapshot que tenha sido compartilhado com você. Por padrão, a cópia é criptografada com uma Chave do KMS compartilhada pelo proprietário do snapshot. No entanto, recomendamos que você crie uma cópia do snapshot compartilhado usando uma Chave do KMS diferente que esteja sob seu controle. Isso protegerá seu acesso ao volume se a Chave do KMS original estiver comprometida ou se o proprietário revogar a Chave do KMS por algum motivo. Para obter mais informações, consulte [Cópia de snapshot e criptografia \(p. 1319\)](#).

Migrar dados entre volumes criptografados e não criptografados

Quando você tem acesso a volumes criptografados e não criptografados, pode transferir livremente dados entre eles. O EC2 realiza as operações de criptografia ou descriptografia de forma transparente.

Por exemplo: use o comando robocopy para copiar os dados. No comando a seguir, os dados de origem estão localizados em D:\ e o volume de destino está montado em E:\.

```
PS C:\> robocopy D:\sourcefolder E:\destinationfolder /e /copyall /eta
```

É recomendável usar pastas, em vez de copiar um volume inteiro, para evitar possíveis problemas com pastas ocultas.

Resultados da criptografia

A tabela a seguir descreve o resultado da criptografia para cada combinação possível de configurações.

A criptografia está ativada?	A criptografia está ativada por padrão?	Origem do volume	Padrão (nenhuma chave gerenciada pelo cliente especificada)	Personalizado (chave gerenciada pelo cliente especificada)
Não	Não	Novo volume (vazio)	Não criptografado	N/D
Não	Não	Snapshot não criptografado pertencente a você	Não criptografado	
Não	Não	Snapshot criptografado pertencente a você	Criptografado pela mesma chave	
Não	Não	Snapshot não criptografado compartilhado com você	Não criptografado	
Não	Não	Snapshot criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente*	
Sim	Não	Novo volume	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Não	Snapshot não criptografado pertencente a você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Não	Snapshot criptografado pertencente a você	Criptografado pela mesma chave	
Sim	Não	Snapshot não criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Não	Snapshot criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Não	Sim	Novo volume (vazio)	Criptografado por chave padrão	N/D

A criptografia está ativada?	A criptografia está ativada por padrão?	Origem do volume	Padrão (nenhuma chave gerenciada pelo cliente especificada)	Personalizado (chave gerenciada pelo cliente especificada)
			gerenciada pelo cliente	
Não	Sim	Snapshot não criptografado pertencente a você	Criptografado por chave padrão gerenciada pelo cliente	
Não	Sim	Snapshot criptografado pertencente a você	Criptografado pela mesma chave	
Não	Sim	Snapshot não criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Não	Sim	Snapshot criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Sim	Novo volume	Criptografado por chave padrão gerenciada pelo cliente	Criptografado por uma chave gerenciada pelo cliente especificada
Sim	Sim	Snapshot não criptografado pertencente a você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Sim	Snapshot criptografado pertencente a você	Criptografado pela mesma chave	
Sim	Sim	Snapshot não criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	
Sim	Sim	Snapshot criptografado compartilhado com você	Criptografado por chave padrão gerenciada pelo cliente	

* Esta é a chave gerenciada pelo cliente padrão usada para criptografia do EBS para a conta e região da AWS. Por padrão, é uma Chave gerenciada pela AWS exclusiva para o EBS, ou você pode especificar uma chave gerenciada pelo cliente. Para obter mais informações, consulte [Padrão Chave do KMS para criptografia EBS \(p. 1425\)](#).

** Esta é uma chave gerenciada pelo cliente especificada para o volume no momento do lançamento. Essa chave gerenciada pelo cliente é usada em vez da chave gerenciada pelo cliente padrão para a conta e a região da AWS.

Configurar padrões de criptografia usando a API e a CLI

Você pode gerenciar a criptografia por padrão e a Chave do KMS padrão usando os comandos da CLI e ações de API a seguir.

Ação de API	Comando da CLI	Descrição
DisableEbsEncryptionByDefault	disable-ebs-encryption-by-default	Desativa a criptografia por padrão.
EnableEbsEncryptionByDefault	enable-ebs-encryption-by-default	Ativa a criptografia por padrão.
GetEbsDefaultKmsKeyId	get-ebs-default-kms-key-id	Descreve a Chave do KMS padrão.
GetEbsEncryptionByDefault	get-ebs-encryption-by-default	Indica se a criptografia por padrão está ativada.
ModifyEbsDefaultKmsKeyId	modify-ebs-default-kms-key-id	Altera a Chave do KMS padrão usada para criptografar volumes do EBS.
ResetEbsDefaultKmsKeyId	reset-ebs-default-kms-key-id	Redefine a Chave gerenciada pela AWS como chave do KMS padrão usada para criptografar volumes do EBS.

Restauração rápida de snapshots do Amazon EBS

A restauração rápida de snapshots do Amazon EBS permite criar um volume de um snapshot que está totalmente inicializado na criação. Isso elimina a latência das operações de E/S em um bloco quando ele é acessado pela primeira vez. Os volumes criados usando a restauração rápida de snapshots viabilizam instantaneamente toda a sua performance provisionada.

Para iniciar, habilite a restauração rápida de snapshots específicos em zonas de disponibilidade determinadas. Cada par de snapshots e zonas de disponibilidade refere-se a uma restauração rápida de snapshot. Ao criar um volume de um desses snapshots em uma de suas zonas de disponibilidade habilitadas, o volume é restaurado usando a restauração rápida de snapshot.

A restauração rápida do snapshot deve ser habilitada explicitamente por snapshot. Se você criar um novo snapshot de um volume que foi restaurado de um snapshot habilitado para restauração rápida, o novo snapshot não será ativado automaticamente para restauração rápida de snapshots. É necessário habilitá-lo explicitamente para o novo snapshot.

Você pode habilitar a restauração rápida de snapshots que você possui e de snapshots públicos e privados compartilhados com você.

Tópicos

- [Cotas de restauração rápida de snapshots \(p. 1435\)](#)
- [Estados da restauração rápida de snapshots \(p. 1435\)](#)
- [Créditos de criação de volume \(p. 1435\)](#)
- [Gerenciar a restauração rápida de snapshots \(p. 1436\)](#)

- [Exibir snapshots com restauração rápida de snapshot ativada \(p. 1437\)](#)
- [Exibir volumes restaurados usando restauração rápida de snapshot \(p. 1437\)](#)
- [Monitorar a restauração rápida de snapshot \(p. 1438\)](#)
- [Definição de preço e cobrança \(p. 1438\)](#)

Cotas de restauração rápida de snapshots

Você pode habilitar até 50 snapshots para restauração rápida de snapshots por região. A cota se aplica aos snapshots que você possui e aos snapshots compartilhados com você. Se você habilitar a restauração rápida de um snapshot compartilhado com você, ela será contada em sua cota de restauração rápida de snapshots. Ela não será contada na cota de restauração rápida de snapshots do proprietário do snapshot.

Estados da restauração rápida de snapshots

Depois que você habilita a restauração rápida para um snapshot, ela pode estar em um dos estados a seguir.

- **enabling** — foi feita uma solicitação para habilitar a restauração rápida de snapshots.
- **optimizing** — a restauração rápida de snapshots está sendo habilitada. Demora 60 minutos por TiB para otimizar um snapshot. Os snapshots nesse estado oferecem alguns benefícios de performance ao restaurar volumes.
- **enabled** — a restauração rápida de snapshots está habilitada. Os snapshots nesse estado oferecem o benefício de performance total ao restaurar volumes.
- **disabling** — foi feita uma solicitação para desabilitar a restauração rápida de snapshots ou houve falha em uma solicitação para habilitar a restauração rápida de snapshots.
- **disabled** — a restauração rápida de snapshots está desabilitada. Você pode reabilitar a restauração rápida de snapshots, se necessário.

Créditos de criação de volume

O número de volumes que recebem todo o benefício da performance da restauração rápida de snapshots é determinado pelos créditos de criação de volume para o snapshot. Existe um bucket de crédito por snapshot por zona de disponibilidade. Cada volume criado a partir de um snapshot com restauração rápida de snapshots consome um crédito do bucket de crédito. Se você criar um volume, mas houver menos de um crédito no bucket, o volume será criado sem o benefício da restauração rápida de snapshots.

Quando você habilita a restauração rápida de snapshots para um snapshot compartilhado com você, você obtém um bucket de crédito separado para o snapshot compartilhado em sua conta. Se você criar volumes do snapshot compartilhado, os créditos serão consumidos de seu bucket de crédito; eles não serão consumidos do bucket de crédito do proprietário do snapshot.

O tamanho do bucket de crédito depende do tamanho do snapshot, não do tamanho dos volumes criados a partir do snapshot. O tamanho do bucket de crédito de cada snapshot é calculado da seguinte forma:

```
MAX (1, MIN (10, FLOOR(1024/snapshot_size_gib)))
```

Ao consumir créditos, o bucket de crédito é reabastecido com o tempo. A velocidade de reabastecimento de cada bucket de crédito é calculada da seguinte forma:

```
MIN (10, 1024/snapshot_size_gib)
```

Por exemplo, se você habilitar a restauração rápida de um snapshot que tenha 100 GiB de tamanho, o tamanho máximo do bucket de crédito será 10 créditos e a velocidade de reabastecimento será de 10

créditos por hora. Quando o bucket de crédito estiver cheio, você poderá criar 10 volumes inicializados simultaneamente a partir desse snapshot.

É possível usar métricas do CloudWatch para monitorar o tamanho dos buckets de crédito e o número de créditos disponíveis em cada bucket. Para obter mais informações, consulte [Métricas de restauração rápida do snapshot \(p. 1477\)](#).

Após criar um volume de um snapshot com a restauração rápida de snapshots habilitada, será possível descrever o volume usando [describe-volumes](#) e verificar o campo `fastRestored` na saída para determinar se o volume foi criado como um volume inicializado usando a restauração rápida de snapshots.

Gerenciar a restauração rápida de snapshots

Por padrão, a restauração rápida de snapshots está desabilitada para um snapshot. Você pode habilitar ou desabilitar a restauração rápida de snapshots para snapshots que você possui e que são compartilhados com você. Quando você habilita ou desabilita a restauração rápida de snapshots para um snapshot, as alterações se aplicam somente à sua conta.

Note

Quando você habilita a restauração rápida de snapshots para um snapshot, sua conta é cobrada por cada minuto em que a restauração rápida de snapshot está habilitada em uma determinada zona de disponibilidade. As cobranças são proporcionais, com um mínimo de uma hora.

Quando você exclui um snapshot que você possui, a restauração rápida de snapshots é automaticamente desabilitada para esse snapshot em sua conta. Se você habilitou a restauração rápida de snapshots para um snapshot compartilhado com você, e o proprietário do snapshot exclui-lo ou descompartilhá-lo, a restauração rápida de snapshots será automaticamente desabilitada para o snapshot compartilhado em sua conta.

Se você habilitou a restauração rápida de snapshots para um snapshot compartilhado com você e ele for criptografado usando uma CMK personalizada, a restauração rápida de snapshots não será desabilitada automaticamente para o snapshot quando o proprietário do snapshot revogar seu acesso à CMK personalizada. Você deve desabilitar manualmente a restauração rápida de snapshots para esse snapshot.

Use o procedimento a seguir para habilitar ou desabilitar a restauração rápida de snapshots para um snapshot que você possui ou para um snapshot compartilhado com você.

Como habilitar ou desabilitar a restauração rápida de snapshot

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot.
4. Selecione Actions (Ações), Manage Fast Snapshot Restore (Gerenciar restauração rápida de snapshots).
5. Marque ou desmarque as zonas de disponibilidade e clique em Save (Salvar).
6. Para monitorar o estado da restauração rápida de snapshots ao ser habilitada, consulte [Fast Snapshot Restore \(restauração rápida de snapshots\)](#) na guia Description (Descrição).

Note

Depois que você habilitar a restauração rápida para um snapshot, ele entrará no estado `optimizing`. Os snapshots que estão no estado `optimizing` oferecem alguns benefícios de performance ao usá-los para restaurar volumes. Eles passam a oferecer os benefícios de performance total da restauração rápida de snapshots somente depois de entrarem no estado `enabled`.

Para gerenciar a restauração rápida de snapshots usando a AWS CLI

- [enable-fast-snapshot-restores](#)
- [disable-fast-snapshot-restores](#)
- [describe-fast-snapshot-restores](#)

Exibir snapshots com restauração rápida de snapshot ativada

Use o procedimento a seguir para exibir o estado da restauração rápida de snapshot para um snapshot que você possui ou para um snapshot compartilhado com você.

Como exibir o estado da restauração rápida do snapshot usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Snapshots.
3. Selecione o snapshot.
4. Na guia Description (Descrição), consulte Fast Snapshot Restore (Restauração rápida de snapshot), que indica o estado da restauração rápida do snapshot. Por exemplo, ela pode mostrar um estado de "2 zonas de disponibilidade em otimização" ou "2 zonas de disponibilidade habilitadas".

Como exibir snapshots com restauração rápida habilitada com a AWS CLI

Use o comando [describe-fast-snapshot-restores](#) para descrever os snapshots habilitados para restauração rápida.

```
aws ec2 describe-fast-snapshot-restores --filters Name=state,Values=enabled
```

A seguir está um exemplo de saída.

```
{  
    "FastSnapshotRestores": [  
        {  
            "SnapshotId": "snap-0e946653493cb0447",  
            "AvailabilityZone": "us-east-2a",  
            "State": "enabled",  
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state transition",  
            "OwnerId": "123456789012",  
            "EnablingTime": "2020-01-25T23:57:49.596Z",  
            "OptimizingTime": "2020-01-25T23:58:25.573Z",  
            "EnabledTime": "2020-01-25T23:59:29.852Z"  
        },  
        {  
            "SnapshotId": "snap-0e946653493cb0447",  
            "AvailabilityZone": "us-east-2b",  
            "State": "enabled",  
            "StateTransitionReason": "Client.UserInitiated - Lifecycle state transition",  
            "OwnerId": "123456789012",  
            "EnablingTime": "2020-01-25T23:57:49.596Z",  
            "OptimizingTime": "2020-01-25T23:58:25.573Z",  
            "EnabledTime": "2020-01-25T23:59:29.852Z"  
        }  
    ]  
}
```

Exibir volumes restaurados usando restauração rápida de snapshot

Ao criar um volume de um snapshot habilitado para restauração rápida na zona de disponibilidade para o volume, ele é restaurado usando a restauração rápida de snapshot.

Use o comando [describe-volumes](#) para exibir volumes criados a partir de um snapshot habilitado para restauração rápida.

```
aws ec2 describe-volumes --filters Name=fast-restored,Values=true
```

A seguir está um exemplo de saída.

```
{  
    "Volumes": [  
        {  
            "Attachments": [],  
            "AvailabilityZone": "us-east-2a",  
            "CreateTime": "2020-01-26T00:34:11.093Z",  
            "Encrypted": true,  
            "KmsKeyId": "arn:aws:kms:us-west-2:123456789012:key/8c5b2c63-b9bc-45a3-a87a-5513e232e843",  
            "Size": 20,  
            "SnapshotId": "snap-0e946653493cb0447",  
            "State": "available",  
            "VolumeId": "vol-0d371921d4ca797b0",  
            "Iops": 100,  
            "VolumeType": "gp2",  
            "FastRestored": true  
        }  
    ]  
}
```

Monitorar a restauração rápida de snapshot

O Amazon EBS emite eventos do Amazon CloudWatch quando o estado de restauração de um snapshot é alterado. Para obter mais informações, consulte [Eventos de restauração rápida do snapshot do EBS \(p. 1487\)](#).

Definição de preço e cobrança

Você será cobrado por cada minuto em que a restauração rápida de snapshots estiver habilitada para um snapshot em uma determinada zona de disponibilidade. As cobranças são divididas com um mínimo de uma hora.

Por exemplo, se você habilitar a restauração rápida de snapshots para um snapshot em `US-East-1a` por um mês (30 dias), será cobrado 540 USD (1 snapshot x 1 AZ x 720 horas x \$0.75 por hora). Se você habilitar a restauração rápida de snapshots para dois snapshots em `us-east-1a`, `us-east-1b`, e `us-east-1c` para o mesmo período, você será cobrado 3.240 USD (2 snapshots x 3 AZs x 720 horas x \$0.75 por hora).

Se você habilitar a restauração rápida de snapshots para um snapshot público ou privado compartilhado com você, sua conta será cobrada. O proprietário do snapshot não será cobrado. Quando um snapshot compartilhado com você é excluído ou não compartilhado pelo proprietário do snapshot, a restauração rápida do snapshots é desabilitada para o snapshot em sua conta, e o faturamento é interrompido.

Para obter mais informações, consulte [Definição de preço do Amazon EBS](#).

Amazon EBS e NVMe em instâncias Windows

Os volumes do EBS são expostos como dispositivos de blocos NVMe em instâncias criadas no [sistema Nitro \(p. 154\)](#). Quando você anexa um volume à instância, você inclui um nome de dispositivo para o volume. Esse nome de dispositivo é usado pelo Amazon EC2. O driver do dispositivo de blocos da instância atribui o nome real do volume ao montá-lo, e o nome atribuído pode ser diferente do nome usado pelo Amazon EC.

As garantias de performance do EBS declaradas em [Detalhes do produto Amazon EBS](#) são válidas, independentemente da interface de dispositivo de bloco.

Tópicos

- [Instalar ou atualizar o driver NVMe \(p. 1439\)](#)
- [Identificar o dispositivo EBS \(p. 1439\)](#)
- [Trabalhar com volumes de NVMe do EBS \(p. 1440\)](#)
- [Tempo limite de operação de E/S \(p. 1440\)](#)

Instalar ou atualizar o driver NVMe

As AMIs do Windows da AWS para Windows Server 2008 R2 ou posterior incluem o driver NVMe da AWS. Se você não estiver usando as AMIs do Windows da AWS mais recentes fornecidas pela Amazon, consulte [Instalar ou atualizar drivers AWS NVMe \(p. 580\)](#).

Identificar o dispositivo EBS

O EBS usa virtualização de E/S de raiz única (SR-IOV - single-root I/O virtualization) para fornecer anexos de volume em instâncias baseadas em Nitro usando a especificação NVMe. Esses dispositivos dependem dos drivers NVMe padrão no sistema operacional. Normalmente, esses drivers descobrem dispositivos anexados verificando o barramento PCI durante a inicialização da instância e cria nós de dispositivo com base na ordem em que os dispositivos respondem, não em como os dispositivos são especificados no mapeamento de dispositivos de blocos. Além disso, o nome de dispositivo atribuído pelo driver de dispositivo de bloco pode ser diferente do nome especificado no mapeamento de dispositivos de blocos.

O exemplo a seguir mostra o comando e a saída para um volume anexado durante o lançamento da instância. Observe que o nome do dispositivo NVMe não inclui o prefixo `/dev/`.

O exemplo a seguir mostra o comando e a saída para um volume anexado após o lançamento da instância. Observe que o nome do dispositivo NVMe inclui o prefixo `/dev/`.

Windows Server 2008 R2 e posteriores

Você também pode executar o comando `ebsnvme-id` para mapear o número do disco do dispositivo NVMe para um ID de volume e nome de dispositivo do EBS. Por padrão, todos os dispositivos NVMe do EBS estão enumerados. Você pode passar um número de disco para enumerar informações de um dispositivo específico. O `ebsnvme-id` está incluído nas AMIs do Windows Server mais recentes fornecidas pela AWS localizadas em `C:\PROGRAMDATA\AMAZON\Tools`.

Você também pode fazer download do [ebsnvme-id.zip](#) e extrair o conteúdo para a sua instância do Amazon EC2, a fim de obter acesso ao `ebsnvme-id.exe`.

```
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-0d6d7ee9f6e471a7f
Device Name: sda1

Disk Number: 1
Volume ID: vol-03a26248ff39b57cf
Device Name: xvdd

Disk Number: 2
Volume ID: vol-038bd1c629aa125e6
Device Name: xvde

Disk Number: 3
Volume ID: vol-034f9d29ec0b64c89
Device Name: xvdb
```

```
Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
PS C:\Users\Administrator\Desktop> ebsnvme-id.exe 4
Disk Number: 4
Volume ID: vol-03e2dbe464b66f0a1
Device Name: xvdc
```

Trabalhar com volumes de NVMe do EBS

As AMIs do Windows da AWS mais recentes contêm o driver NVMe da AWS exigido por tipos de instância que expõem volumes do EBS como dispositivos de bloco de NVMe. No entanto, se você redimensionar seu volume raiz em um sistema Windows, será necessário fazer a varredura novamente do volume para que a alteração seja refletida na instância. Se você iniciou sua instância de uma AMI diferente, ela pode não conter o driver NVMe da AWS necessário. Se a sua instância não contiver o driver NVMe da AWS mais recente, você precisará instalá-lo. Para obter mais informações, consulte [AWS Drivers NVMe para instâncias do Windows \(p. 580\)](#).

Tempo limite de operação de E/S

A maioria dos sistemas operacionais especifica um tempo limite para as operações de E/S enviadas aos dispositivos NVMe. Nos sistemas do Windows, o tempo limite padrão é de 60 segundos e o máximo é de 255 segundos. Você pode modificar a configuração de registro de classe de disco `TimeoutValue` usando o procedimento descrito em [Entradas de registro para drivers de Miniport de SCSI](#).

Instâncias otimizadas para Amazon EBS

Uma instância otimizada para o Amazon EBS usa uma pilha de configuração otimizada e fornece capacidade adicional dedicada para E/S do Amazon EBS. Essa otimização proporciona a melhor performance para seus volumes do EBS ao minimizar a contenção entre a E/S do Amazon EBS e outro tráfego de sua instância.

Instâncias otimizadas para o EBS oferecem largura de banda dedicada para o Amazon EBS. Quando anexados a uma instância otimizada para o EBS, os volumes SSD de uso geral (`gp2` e `gp3`) fornecem performance básica e intermitente 99,9% do tempo, e os volumes SSD de IOPS provisionadas (`io1` e `io2`) fornecem sua performance provisionada 99,9% do tempo. Tanto o HDD otimizado para taxa de transferência (`st1`) quanto o HDD a frio (`sc1`) garantem a consistência de performance de 90% da taxa de transferência intermitente durante 99% do tempo. Períodos não compatíveis são distribuídos com uniformidade aproximada, destinando 99% da taxa de transferência total esperada a cada hora. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#).

Tópicos

- [Tipos de instâncias compatíveis \(p. 1440\)](#)
- [Obtenha a máxima performance \(p. 1455\)](#)
- [Exibir tipos de instâncias compatíveis com a otimização do EBS \(p. 1455\)](#)
- [Habilitação da otimização do EBS na execução \(p. 1456\)](#)
- [Habilitar a otimização do EBS para uma instância existente \(p. 1457\)](#)

Tipos de instâncias compatíveis

As tabelas a seguir mostram quais tipos de instância oferecem suporte à otimização do EBS. Elas incluem a largura de banda dedicada ao Amazon EBS, a taxa de transferência máxima normal agregada que pode ser atingida nessa conexão com uma workload de leitura de transmissão e tamanho de E/S de 128 KiB, além de número máximo de IOPS para o qual a instância oferece suporte se você estiver usando um tamanho de E/S de 16 KiB. Escolha uma instância otimizada para EBS que forneça uma taxa de

transferência do Amazon EBS mais dedicada do que o necessário para sua aplicação. Caso contrário, a conexão entre o Amazon EBS e o Amazon EC2 pode se tornar um gargalo de performance.

Otimizadas para EBS por padrão

A tabela a seguir lista os tipos de instância que oferecem suporte à otimização do EBS e essa otimização está habilitada por padrão. Não é necessário habilitar a otimização para EBS, e nada ocorrerá se você desabilitá-la.

Note

Também é possível visualizar essas informações de maneira programática usando a AWS CLI. Para obter mais informações, consulte [Exibir tipos de instâncias compatíveis com a otimização do EBS \(p. 1455\)](#).

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
c4.large	500	62.5	4.000
c4.xlarge	750	93,75	6.000
c4.2xlarge	1.000	125	8.000
c4.4xlarge	2.000	250	16.000
c4.8xlarge	4.000	500	32.000
c5.large *	4.750	593,75	20.000
c5.xlarge *	4.750	593,75	20.000
c5.2xlarge *	4.750	593,75	20.000
c5.4xlarge	4.750	593,75	20.000
c5.9xlarge	9.500	1.187,5	40.000
c5.12xlarge	9.500	1.187,5	40.000
c5.18xlarge	19.000	2.375	80.000
c5.24xlarge	19.000	2.375	80.000
c5.metal	19.000	2.375	80.000
c5a.large *	3.170	396	13.300
c5a.xlarge *	3.170	396	13.300
c5a.2xlarge *	3.170	396	13.300
c5a.4xlarge *	3.170	396	13.300
c5a.8xlarge	3.170	396	13.300
c5a.12xlarge	4.750	594	20.000
c5a.16xlarge	6.300	788	26.700
c5a.24xlarge	9.500	1.188	40.000

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
c5ad.large *	3.170	396	13.300
c5ad.xlarge *	3.170	396	13.300
c5ad.2xlarge *	3.170	396	13.300
c5ad.4xlarge *	3.170	396	13.300
c5ad.8xlarge	3.170	396	13.300
c5ad.12xlarge	4.750	594	20.000
c5ad.16xlarge	6.300	788	26.700
c5ad.24xlarge	9.500	1.188	40.000
c5d.large *	4.750	593,75	20.000
c5d.xlarge *	4.750	593,75	20.000
c5d.2xlarge *	4.750	593,75	20.000
c5d.4xlarge	4.750	593,75	20.000
c5d.9xlarge	9.500	1.187,5	40.000
c5d.12xlarge	9.500	1.187,5	40.000
c5d.18xlarge	19.000	2.375	80.000
c5d.24xlarge	19.000	2.375	80.000
c5d.metal	19.000	2.375	80.000
c5n.large *	4.750	593,75	20.000
c5n.xlarge *	4.750	593,75	20.000
c5n.2xlarge *	4.750	593,75	20.000
c5n.4xlarge	4.750	593,75	20.000
c5n.9xlarge	9.500	1.187,5	40.000
c5n.18xlarge	19.000	2.375	80.000
c5n.metal	19.000	2.375	80.000
d2.xlarge	750	93,75	6.000
d2.2xlarge	1.000	125	8.000
d2.4xlarge	2.000	250	16.000
d2.8xlarge	4.000	500	32.000
d3.xlarge *	2.800	350	15.000
d3.2xlarge *	2.800	350	15.000

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
d3.4xlarge	2.800	350	15.000
d3.8xlarge	5.000	625	30.000
d3en.xlarge *	2.800	350	15.000
d3en.2xlarge *	2.800	350	15.000
d3en.4xlarge	2.800	350	15.000
d3en.8xlarge	5.000	625	30.000
d3en.12xlarge	7.000	875	40.000
f1.2xlarge	1.700	212,5	12.000
f1.4xlarge	3.500	437,5	44.000
f1.16xlarge	14.000	1.750	75.000
g3s.xlarge	850	106,25	5.000
g3.4xlarge	3.500	437,5	20.000
g3.8xlarge	7.000	875	40.000
g3.16xlarge	14.000	1.750	80.000
g4ad.xlarge *	3.170	396,25	13.333
g4ad.2xlarge *	3.170	396,25	13.333
g4ad.4xlarge *	3.170	396,25	13.333
g4ad.8xlarge	3.170	396,25	13.333
g4ad.16xlarge	6.300	787,5	26.667
g4dn.xlarge *	3.500	437,5	20.000
g4dn.2xlarge *	3.500	437,5	20.000
g4dn.4xlarge	4.750	593,75	20.000
g4dn.8xlarge	9.500	1.187,5	40.000
g4dn.12xlarge	9.500	1.187,5	40.000
g4dn.16xlarge	9.500	1.187,5	40.000
g4dn.metal	19.000	2.375	80.000
h1.2xlarge	1.750	218,75	12.000
h1.4xlarge	3.500	437,5	20.000
h1.8xlarge	7.000	875	40.000
h1.16xlarge	14.000	1.750	80.000

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Otimização de EBS

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
i3.large	425	53,13	3000
i3.xlarge	850	106,25	6000
i3.2xlarge	1.700	212,5	12.000
i3.4xlarge	3.500	437,5	16.000
i3.8xlarge	7.000	875	32.500
i3.16xlarge	14.000	1.750	65.000
i3.metal	19.000	2.375	80.000
i3en.large *	4.750	593,75	20.000
i3en.xlarge *	4.750	593,75	20.000
i3en.2xlarge *	4.750	593,75	20.000
i3en.3xlarge *	4.750	593,75	20.000
i3en.6xlarge	4.750	593,75	20.000
i3en.12xlarge	9.500	1.187,5	40.000
i3en.24xlarge	19.000	2.375	80.000
i3en.metal	19.000	2.375	80.000
m4.large	450	56,25	3.600
m4.xlarge	750	93,75	6.000
m4.2xlarge	1.000	125	8.000
m4.4xlarge	2.000	250	16.000
m4.10xlarge	8.000	500	32.000
m4.16xlarge	10.000	1.250	65.000
m5.large *	4.750	593,75	18.750
m5.xlarge *	4.750	593,75	18.750
m5.2xlarge *	4.750	593,75	18.750
m5.4xlarge	4.750	593,75	18.750
m5.8xlarge	6.800	850	30.000
m5.12xlarge	9.500	1.187,5	40.000
m5.16xlarge	13.600	1.700	60.000
m5.24xlarge	19.000	2.375	80.000
m5.metal	19.000	2.375	80.000

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Otimização de EBS

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
m5a.large *	2.880	360	16.000
m5a.xlarge *	2.880	360	16.000
m5a.2xlarge *	2.880	360	16.000
m5a.4xlarge	2.880	360	16.000
m5a.8xlarge	4.750	593,75	20.000
m5a.12xlarge	6.780	847,5	30.000
m5a.16xlarge	9.500	1.187,50	40.000
m5a.24xlarge	13.570	1.696,25	60.000
m5ad.large *	2.880	360	16.000
m5ad.xlarge *	2.880	360	16.000
m5ad.2xlarge *	2.880	360	16.000
m5ad.4xlarge	2.880	360	16.000
m5ad.8xlarge	4.750	593,75	20.000
m5ad.12xlarge	6.780	847,5	30.000
m5ad.16xlarge	9.500	1.187,5	40.000
m5ad.24xlarge	13.570	1.696,25	60.000
m5d.large *	4.750	593,75	18.750
m5d.xlarge *	4.750	593,75	18.750
m5d.2xlarge *	4.750	593,75	18.750
m5d.4xlarge	4.750	593,75	18.750
m5d.8xlarge	6.800	850	30.000
m5d.12xlarge	9.500	1.187,5	40.000
m5d.16xlarge	13.600	1.700	60.000
m5d.24xlarge	19.000	2.375	80.000
m5d.metal	19.000	2.375	80.000
m5dn.large *	4.750	593,75	18.750
m5dn.xlarge *	4.750	593,75	18.750
m5dn.2xlarge *	4.750	593,75	18.750
m5dn.4xlarge	4.750	593,75	18.750
m5dn.8xlarge	6.800	850	30.000

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Otimização de EBS

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
m5dn.12xlarge	9.500	1.187,5	40.000
m5dn.16xlarge	13.600	1.700	60.000
m5dn.24xlarge	19.000	2.375	80.000
m5dn.metal	19.000	2.375	80.000
m5n.large *	4.750	593,75	18.750
m5n.xlarge *	4.750	593,75	18.750
m5n.2xlarge *	4.750	593,75	18.750
m5n.4xlarge	4.750	593,75	18.750
m5n.8xlarge	6.800	850	30.000
m5n.12xlarge	9.500	1.187,5	40.000
m5n.16xlarge	13.600	1.700	60.000
m5n.24xlarge	19.000	2.375	80.000
m5n.metal	19.000	2.375	80.000
m5zn.large *	3.170	396,25	13.333
m5zn.xlarge *	3.170	396,25	13.333
m5zn.2xlarge	3.170	396,25	13.333
m5zn.3xlarge	4.750	593,75	20.000
m5zn.6xlarge	9.500	1187,5	40.000
m5zn.12xlarge	19.000	2.375	80.000
m5zn.metal	19.000	2.375	80.000
m6i.large *	10.000	1.250	40.000
m6i.xlarge *	10.000	1.250	40.000
m6i.2xlarge *	10.000	1.250	40.000
m6i.4xlarge *	10.000	1.250	40.000
m6i.8xlarge	10.000	1.250	40.000
m6i.12xlarge	15.000	1.875	60.000
m6i.16xlarge	20.000	2.500	80.000
m6i.24xlarge	30.000	3.750	120.000
m6i.32xlarge	40.000	5.000	160.000
p2.xlarge	750	93,75	6.000

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Otimização de EBS

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
p2.8xlarge	5.000	625	32.500
p2.16xlarge	10.000	1.250	65.000
p3.2xlarge	1.750	218,75	10.000
p3.8xlarge	7.000	875	40.000
p3.16xlarge	14.000	1.750	80.000
p3dn.24xlarge	19.000	2.375	80.000
r4.large	425	53,13	3.000
r4.xlarge	850	106,25	6.000
r4.2xlarge	1.700	212,5	12.000
r4.4xlarge	3.500	437,5	18.750
r4.8xlarge	7.000	875	37.500
r4.16xlarge	14.000	1.750	75.000
r5.large *	4.750	593,75	18.750
r5.xlarge *	4.750	593,75	18.750
r5.2xlarge *	4.750	593,75	18.750
r5.4xlarge	4.750	593,75	18.750
r5.8xlarge	6.800	850	30.000
r5.12xlarge	9.500	1.187,5	40.000
r5.16xlarge	13.600	1.700	60.000
r5.24xlarge	19.000	2.375	80.000
r5.metal	19.000	2.375	80.000
r5a.large *	2.880	360	16.000
r5a.xlarge *	2.880	360	16.000
r5a.2xlarge *	2.880	360	16.000
r5a.4xlarge	2.880	360	16.000
r5a.8xlarge	4.750	593,75	20.000
r5a.12xlarge	6.780	847,5	30.000
r5a.16xlarge	9.500	1.187,5	40.000
r5a.24xlarge	13.570	1.696,25	60.000
r5ad.large *	2.880	360	16.000

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
r5ad.xlarge *	2.880	360	16.000
r5ad.2xlarge *	2.880	360	16.000
r5ad.4xlarge	2.880	360	16.000
r5ad.8xlarge	4.750	593,75	20.000
r5ad.12xlarge	6.780	847,5	30.000
r5ad.16xlarge	9.500	1.187,5	40.000
r5ad.24xlarge	13.570	1.696,25	60.000
r5b.large *	10.000	1.250	43.333
r5b.xlarge *	10.000	1.250	43.333
r5b.2xlarge *	10.000	1.250	43.333
r5b.4xlarge	10.000	1.250	43.333
r5b.8xlarge	20.000	2.500	86.667
r5b.12xlarge	30.000	3.750	130.000
r5b.16xlarge	40.000	5.000	173.333
r5b.24xlarge	60.000	7.500	260.000
r5b.metal	60.000	7.500	260.000
r5d.large *	4.750	593,75	18.750
r5d.xlarge *	4.750	593,75	18.750
r5d.2xlarge *	4.750	593,75	18.750
r5d.4xlarge	4.750	593,75	18.750
r5d.8xlarge	6.800	850	30.000
r5d.12xlarge	9.500	1.187,5	40.000
r5d.16xlarge	13.600	1.700	60.000
r5d.24xlarge	19.000	2.375	80.000
r5d.metal	19.000	2.375	80.000
r5dn.large *	4.750	593,75	18.750
r5dn.xlarge *	4.750	593,75	18.750
r5dn.2xlarge *	4.750	593,75	18.750
r5dn.4xlarge	4.750	593,75	18.750
r5dn.8xlarge	6.800	850	30.000

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
r5dn.12xlarge	9.500	1.187,5	40.000
r5dn.16xlarge	13.600	1.700	60.000
r5dn.24xlarge	19.000	2.375	80.000
r5dn.metal	19.000	2.375	80.000
r5n.large *	4.750	593,75	18.750
r5n.xlarge *	4.750	593,75	18.750
r5n.2xlarge *	4.750	593,75	18.750
r5n.4xlarge	4.750	593,75	18.750
r5n.8xlarge	6.800	850	30.000
r5n.12xlarge	9.500	1.187,5	40.000
r5n.16xlarge	13.600	1.700	60.000
r5n.24xlarge	19.000	2.375	80.000
r5n.metal	19.000	2.375	80.000
t3.nano *	2.085	260,57	11.800
t3.micro *	2.085	260,57	11.800
t3.small *	2.085	260,57	11.800
t3.medium *	2.085	260,57	11.800
t3.large *	2.780	347,5	15.700
t3.xlarge *	2.780	347,5	15.700
t3.2xlarge *	2.780	347,5	15.700
t3a.nano *	2.085	260,57	11.800
t3a.micro *	2.085	260,57	11.800
t3a.small *	2.085	260,57	11.800
t3a.medium *	2.085	260,57	11.800
t3a.large *	2.780	347,5	15.700
t3a.xlarge *	2.780	347,5	15.700
t3a.2xlarge *	2.780	347,5	15.700
u-6tb1.56xlarge	38.000	4.750	160.000
u-6tb1.112xlarge	38.000	4.750	160.000
u-6tb1.metal	38.000	4.750	160.000

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
u-9tb1.112xlarge	38.000	4.750	160.000
u-9tb1.metal	38.000	4.750	160.000
u-12tb1.112xlarge	38.000	4.750	160.000
u-12tb1.metal	38.000	4.750	160.000
u-18tb1.metal	38.000	4.750	160.000
u-24tb1.metal	38.000	4.750	160.000
x1.16xlarge	7.000	875	40.000
x1.32xlarge	14.000	1.750	80.000
x1e.xlarge	500	62.5	3.700
x1e.2xlarge	1.000	125	7.400
x1e.4xlarge	1.750	218,75	10.000
x1e.8xlarge	3.500	437,5	20.000
x1e.16xlarge	7.000	875	40.000
x1e.32xlarge	14.000	1.750	80.000
z1d.large *	3.170	396,25	13.333
z1d.xlarge *	3.170	396,25	13.333
z1d.2xlarge	3.170	396,25	13.333
z1d.3xlarge	4.750	593,75	20.000
z1d.6xlarge	9.500	1.187,5	40.000
z1d.12xlarge	19.000	2.375	80.000
z1d.metal	19.000	2.375	80.000

* Esses tipos de instância podem dar suporte a uma performance máxima por 30 minutos a cada 24 horas pelo menos. Se você tiver uma workload que exija performance máxima sustentada por mais de 30 minutos, selecione um tipo de instância de acordo com a performance basal como mostrado na tabela a seguir.

Tamanho da instância	Largura de banda da linha de base (Mbps)	Taxa de transferência de linha de base (MB/s, E/S de 128 KiB)	IOPS da linha de base (E/S de 16 KiB)
c5.large	650	81,25	4.000
c5.xlarge	1.150	143,75	6.000
c5.2xlarge	2.300	287,5	10.000

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Otimização de EBS

Tamanho da instância	Largura de banda da linha de base (Mbps)	Taxa de transferência de linha de base (MB/s, E/S de 128 KiB)	IOPS da linha de base (E/S de 16 KiB)
c5a.large	200	25	800
c5a.xlarge	400	50	1.600
c5a.2xlarge	800	100	3.200
c5a.4xlarge	1.580	198	6.600
c5ad.large	200	25	800
c5ad.xlarge	400	50	1.600
c5ad.2xlarge	800	100	3.200
c5ad.4xlarge	1.580	198	6.600
c5d.large	650	81,25	4.000
c5d.xlarge	1.150	143,75	6.000
c5d.2xlarge	2.300	287,5	10.000
c5n.large	650	81,25	4.000
c5n.xlarge	1.150	143,75	6.000
c5n.2xlarge	2.300	287,5	10.000
d3.xlarge	850	106,25	5.000
d3.2xlarge	1.700	212,5	10.000
d3en.large	425	53.125	2.500
d3en.xlarge	850	106,25	5.000
d3en.2xlarge	1.700	212,5	10.000
g4ad.xlarge	400	50	1.700
g4ad.2xlarge	800	100	3.400
g4ad.4xlarge	1.580	197,5	6.700
g4dn.xlarge	950	118,75	3.000
g4dn.2xlarge	1.150	143,75	6.000
i3en.large	577	72,1	3.000
i3en.xlarge	1.154	144,2	6.000
i3en.2xlarge	2.307	288,39	12.000
i3en.3xlarge	3.800	475	15.000
m5.large	650	81,25	3.600
m5.xlarge	1.150	143,75	6.000

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Otimização de EBS

Tamanho da instância	Largura de banda da linha de base (Mbps)	Taxa de transferência de linha de base (MB/s, E/S de 128 KiB)	IOPS da linha de base (E/S de 16 KiB)
m5.2xlarge	2.300	287,5	12.000
m5a.large	650	81,25	3.600
m5a.xlarge	1.085	135,63	6.000
m5a.2xlarge	1.580	197,5	8.333
m5ad.large	650	81,25	3.600
m5ad.xlarge	1.085	135,63	6.000
m5ad.2xlarge	1.580	197,5	8.333
m5d.large	650	81,25	3.600
m5d.xlarge	1.150	143,75	6.000
m5d.2xlarge	2.300	287,5	12.000
m5dn.large	650	81,25	3.600
m5dn.xlarge	1.150	143,75	6.000
m5dn.2xlarge	2.300	287,5	12.000
m5n.large	650	81,25	3.600
m5n.xlarge	1.150	143,75	6.000
m5n.2xlarge	2.300	287,5	12.000
m5zn.large	800	100	3.333
m5zn.xlarge	1.580	195,5	6.667
m6i.large	650	81,25	3.600
m6i.xlarge	1.250	156,25	6.000
m6i.2xlarge	2.500	312,5	12.000
m6i.4xlarge	5.000	625	20.000
r5.large	650	81,25	3.600
r5.xlarge	1.150	143,75	6.000
r5.2xlarge	2.300	287,5	12.000
r5a.large	650	81,25	3.600
r5a.xlarge	1.085	135,63	6.000
r5a.2xlarge	1.580	197,5	8.333
r5ad.large	650	81,25	3.600
r5ad.xlarge	1.085	135,63	6.000

Tamanho da instância	Largura de banda da linha de base (Mbps)	Taxa de transferência de linha de base (MB/s, E/S de 128 KiB)	IOPS da linha de base (E/S de 16 KiB)
r5ad.2xlarge	1.580	197,5	8.333
r5b.large	1.250	156,25	5.417
r5b.xlarge	2.500	312,5	10.833
r5b.2xlarge	5.000	625	21.667
r5d.large	650	81,25	3.600
r5d.xlarge	1.150	143,75	6.000
r5d.2xlarge	2.300	287,5	12.000
r5dn.large	650	81,25	3.600
r5dn.xlarge	1.150	143,75	6.000
r5dn.2xlarge	2.300	287,5	12.000
r5n.large	650	81,25	3.600
r5n.xlarge	1.150	143,75	6.000
r5n.2xlarge	2.300	287,5	12.000
t3.nano	43	5,43	250
t3.micro	87	10,86	500
t3.small	174	21,71	1.000
t3.medium	347	43,43	2.000
t3.large	695	86,86	4.000
t3.xlarge	695	86,86	4.000
t3.2xlarge	695	86,86	4.000
t3a.nano	45	5,63	250
t3a.micro	90	11,25	500
t3a.small	175	21,88	1.000
t3a.medium	350	43,75	2.000
t3a.large	695	86,86	4.000
t3a.xlarge	695	86,86	4.000
t3a.2xlarge	695	86,86	4.000
z1d.large	800	100	3.333
z1d.xlarge	1.580	197,5	6.667

Suporte à otimização do EBS

A tabela a seguir lista os tipos de instância que oferecem suporte à otimização do EBS, mas essa otimização não está habilitada por padrão. É possível habilitar a otimização do EBS ao executar essas instâncias ou após elas estarem em execução. As instâncias devem ter a otimização de EBS habilitada para alcançar o nível de performance descrito. Ao ativar a otimização de EBS para uma instância que não esteja otimizada para EBS, você paga uma pequena taxa adicional por hora pela capacidade dedicada. Para obter informações de definição de preço, consulte Instâncias otimizadas para EBS na [página Definição de preço do Amazon EC2, Definição de preço sob demanda](#).

Note

Também é possível visualizar essas informações de maneira programática usando a AWS CLI. Para obter mais informações, consulte [Exibir tipos de instâncias compatíveis com a otimização do EBS \(p. 1455\)](#).

Tamanho da instância	Largura de banda máxima (Mbps)	Taxa de transferência máxima (MB/s, 128 KiB E/S)	IOPS máxima (16 KiB de E/S)
c1.xlarge	1.000	125	8.000
c3.xlarge	500	62.5	4.000
c3.2xlarge	1.000	125	8.000
c3.4xlarge	2.000	250	16.000
g2.2xlarge	1.000	125	8.000
i2.xlarge	500	62.5	4.000
i2.2xlarge	1.000	125	8.000
i2.4xlarge	2.000	250	16.000
m1.large	500	62.5	4.000
m1.xlarge	1.000	125	8.000
m2.2xlarge	500	62.5	4.000
m2.4xlarge	1.000	125	8.000
m3.xlarge	500	62.5	4.000
m3.2xlarge	1.000	125	8.000
r3.xlarge	500	62.5	4.000
r3.2xlarge	1.000	125	8.000
r3.4xlarge	2.000	250	16.000

As instâncias **i2.8xlarge**, **c3.8xlarge** e **r3.8xlarge** não possuem largura de banda EBS dedicada e, portanto, não oferecem otimização de EBS. Nessas instâncias, o tráfego de rede e o tráfego de Amazon EBS compartilham a mesma interface de rede de 10 gigabits.

Obtenha a máxima performance

Você pode usar as métricas `EBSIOBalance%` e `EBSByteBalance%` para ajudá-lo a determinar se as instâncias estão dimensionadas corretamente. Você pode exibir essas métricas no console do CloudWatch e definir um alarme que é acionado com base nos limites especificados por você. Essas métricas são expressadas como uma porcentagem. As instâncias com uma porcentagem de equilíbrio consistentemente baixa são candidatas à ampliação. As instâncias nas quais a porcentagem de equilíbrio jamais fica abaixo de 100% são candidatas à redução. Para obter mais informações, consulte [Monitorar instâncias usando o CloudWatch \(p. 898\)](#).

As instâncias com mais memória foram projetadas para executar grandes bancos de dados na memória, incluindo implantações de produção do banco de dados na memória SAP HANA na nuvem. Para maximizar a performance do EBS, use instâncias com mais memória com um número par de volumes de `io1` ou `io2` com performance provisionada idêntica. Por exemplo, para workloads pesadas com relação às IOPS, use quatro volumes de `io1` ou `io2` com 40.000 IOPS provisionadas para obter o máximo de 160.000 IOPS de instância. Da mesma forma, para workloads pesadas com relação à taxa de transferência, use seis volumes de `io1` ou `io2` com 48.000 IOPS provisionadas para obter o máximo de 4.750 MB/s de taxa de transferência. Para obter recomendações adicionais, consulte [Configuração de armazenamento para SAP HANA](#).

Considerações

- As instâncias G4dn, I3en, M5a, M5ad, R5a, R5ad, T3, T3a e Z1d lançadas após 26 de fevereiro de 2020 fornecem a performance máxima listada na tabela acima. Para obter a máxima performance de uma instância lançada antes de 26 de fevereiro de 2020, interrompa-a e inicie-a.
- As instâncias C5, C5d, C5n, M5, M5d, M5n, M5dn, R5, R5d, R5n, R5dn e P3dn lançadas após 3 de dezembro de 2019 fornecem a performance máxima listada na tabela acima. Para obter a performance máxima de uma instância lançada antes de 3 de dezembro de 2019, interrompa-a e inicie-a.
- As instâncias `u-6tb1.metal`, `u-9tb1.metal` e `u-12tb1.metal` lançadas após 12 de março de 2020 fornecem a performance indicada na tabela acima. As instâncias desses tipos lançadas antes de 12 de março de 2020 podem fornecer performance menor. Para obter a performance máxima de uma instância lançada antes de 12 de março de 2020, entre em contato com a equipe de conta para atualizar a instância sem custo adicional.

Exibir tipos de instâncias compatíveis com a otimização do EBS

Use a AWS CLI para exibir os tipos de instâncias na região atual que são compatíveis com a otimização do EBS.

Para visualizar os tipos de instância que oferecem suporte à otimização do EBS e que estão ativados por padrão

Use o comando `describe-instance-types` a seguir.

```
C:\> aws ec2 describe-instance-types \
--query 'InstanceTypes[].[InstanceType:InstanceType,"MaxBandwidth(Mb/s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIops,"MaxThroughput(MBps)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=default --output=table
```

Exemplos de resultado para eu-west-1:

DescribeInstanceTypes	

EBSOptimized	InstanceType	MaxBandwidth(Mb/s)	MaxIOPS	MaxThroughput(MB/s)
default	m5dn.8xlarge	6800	30000	850.0
default	m6gd.xlarge	4750	20000	593.75
default	c4.4xlarge	2000	16000	250.0
default	r4.16xlarge	14000	75000	1750.0
default	m5ad.large	2880	16000	360.0
...				

Para exibir os tipos de instância compatíveis com a otimização do EBS e que estão ativados por padrão

Use o comando [describe-instance-types](#) a seguir.

```
C:\> aws ec2 describe-instance-types \
--query 'InstanceTypes[].[{InstanceType: InstanceType, "MaxBandwidth(Mb/s)": :EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps, MaxIOPS: EbsInfo.EbsOptimizedInfo.MaximumIops, "MaxThroughput(MB/s)": :EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}]' \
--filters Name=ebs-info.ebs-optimized-support,Values=supported --output=table
```

Exemplos de resultado para eu-west-1:

DescribeInstanceTypes				
EBSOptimized	InstanceType	MaxBandwidth(Mb/s)	MaxIOPS	MaxThroughput(MB/s)
supported	m2.4xlarge	1000	8000	125.0
supported	i2.2xlarge	1000	8000	125.0
supported	r3.4xlarge	2000	16000	250.0
supported	m3.xlarge	500	4000	62.5
supported	r3.2xlarge	1000	8000	125.0
...				

Habilitação da otimização do EBS na execução

É possível habilitar a otimização para uma instância definindo o atributo para otimização de EBS.

Para ativar a otimização de Amazon EBS ao executar uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Launch Instance (Executar instância).
3. Em Step 1: Choose an Amazon Machine Image (AMI) (Etapa 1: Escolher uma imagem de máquina da Amazon), selecione uma AMI.
4. Em Step 2: Choose an Instance Type (Etapa 2: Escolher um tipo de instância), selecione um tipo de instância que esteja listada como compatível com a otimização para Amazon EBS.
5. Em Step 3: Configure Instance Details (Etapa 3: Configurar detalhes da instância), preencha os campos necessários e escolha Launch as EBS-optimized instance (Executar como instância otimizada para EBS). Se o tipo de instância que você selecionou na etapa anterior não oferecer suporte à otimização para Amazon EBS, essa opção não estará presente. Se o tipo de instância selecionado for

otimizado para Amazon EBS por padrão, essa opção estará selecionada e você não poderá cancelar a seleção.

6. Siga as instruções para concluir o assistente e executar sua instância.

Para habilitar a otimização para EBS ao executar uma instância usando a linha de comando

Você pode usar um dos seguintes comandos com a opção correspondente. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- `run-instances` com `--ebs-optimized` (AWS CLI)
- `New-EC2Instance` com `-EbsOptimized` (AWS Tools for Windows PowerShell)

Habilitar a otimização do EBS para uma instância existente

Você pode ativar ou desativar a otimização para uma instância existente modificando o atributo de instância otimizada para Amazon EBS. Se a instância estiver em execução, você deve interrompê-la primeiro.

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Como habilitar a otimização de EBS para uma instância existente usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias e selecione a instância.
3. Para interromper a instância, escolha Actions (Ações), Instance state (Estado da instância) e Stop instance (Interromper instância). Pode demorar alguns minutos para que a instância pare.
4. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Change instance type (Alterar tipo de instância).
5. Em Change Instance Type (Alterar tipo de instância), execute um dos seguintes procedimentos:
 - Se o tipo de sua instância for otimizado para Amazon EBS por padrão, a opção EBS-optimized (Otimizada para EBS) será selecionada e você não poderá alterar a seleção. Você pode escolher Cancel (Cancelar), pois a otimização para Amazon EBS já está ativada para a instância.
 - Se o tipo de instância for compatível com a otimização para Amazon EBS, escolha EBS-optimized (Otimizada para EBS) e escolha Apply (Aplicar).
 - Se o tipo de instância não oferecer suporte à otimização de Amazon EBS, você não poderá escolher EBS-optimized (Otimizada para EBS). Você pode selecionar um tipo de instância em Instance type (Tipo de instância) que seja compatível com a otimização para Amazon EBS, escolher EBS-optimized (Otimizada para EBS) e Apply (Aplicar).
6. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância).

Como habilitar a otimização de EBS para uma instância existente usando a linha de comando

1. Se a instância estiver em execução, use um dos seguintes comandos para interrompê-la:
 - `stop-instances` (AWS CLI)
 - `Stop-EC2Instance` (AWS Tools for Windows PowerShell)
2. Para habilitar a otimização do EBS, use um dos seguintes comandos com a opção correspondente:
 - `modify-instance-attribute` com `--ebs-optimized` (AWS CLI)

- [Edit-EC2InstanceAttribute com –EbsOptimized \(AWS Tools for Windows PowerShell\)](#)

Performance de volume do Amazon EBS em instâncias Windows

Vários fatores, como as características de E/S e a configuração das instâncias e volumes, podem afetar a performance dos volumes do Amazon EBS. Os clientes que seguem as orientações em nossas páginas de detalhes do produto do Amazon EBS e do Amazon EC2 conseguem ter uma boa performance imediatamente. Contudo, há alguns casos em que talvez seja necessário fazer alguns ajustes para atingir a performance máxima na plataforma. Este tópico discute práticas recomendadas gerais, bem como o ajuste de performance específico de alguns casos de uso. Recomendamos que você ajuste a performance com informações de sua workload real, além da comparação, para determinar sua configuração ideal. Após você entender os conceitos básicos de utilização dos volumes do EBS, é uma boa ideia examinar a performance de E/S necessária e as opções para melhorar a performance do Amazon EBS a fim de atender a esses requisitos.

As atualizações da AWS para a performance de tipos de volume do EBS podem não ter efeito imediato em seus volumes existentes. Para ver a performance completa em um volume anterior, primeiro você pode precisar realizar uma ação `ModifyVolume` nele. Para obter mais informações, consulte [Modificação de tamanho, IOPS ou tipo de um volume do EBS no Windows](#).

Tópicos

- [Dicas de performance do Amazon EBS \(p. 1458\)](#)
- [Características e monitoramento de E/S \(p. 1459\)](#)
- [Inicializar volumes de Amazon EBS \(p. 1463\)](#)
- [Configuração RAID no Windows \(p. 1465\)](#)
- [Comparar volumes do EBS \(p. 1469\)](#)

Dicas de performance do Amazon EBS

Essas dicas representam as melhores práticas para obter a performance ideal de seus volumes do EBS em uma variedade de cenários de usuário.

Usar instâncias otimizadas para EBS

Em instâncias sem suporte para a taxa de transferência otimizada para EBS, o tráfego de rede poderá competir com o tráfego entre sua instância e seus volumes do EBS. Em instâncias otimizadas para EBS, os dois tipos de tráfego são mantidos separados. Algumas configurações de instâncias otimizadas para EBS incorrem um custo extra (como C3, R3 e M3), enquanto outras são sempre otimizadas para EBS sem custo extra (como M4, C4, C5 e D2). Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

Noções básicas de como a performance é calculada

Quando você mede a performance dos volumes do EBS, é importante compreender as unidades de medida envolvidas e como a performance é calculada. Para obter mais informações, consulte [Características e monitoramento de E/S \(p. 1459\)](#).

Noções básicas da workload

Há uma relação entre a performance máxima dos volumes do EBS, o tamanho e o número de operações de E/S e o tempo necessário para que cada ação seja concluída. Cada um desses fatores (performance,

E/S e latência) afeta os outros, e aplicações diferentes são mais sensíveis em relação a um fator do que outros.

Esteja ciente da penalidade de performance ao inicializar volumes de snapshots

Há um aumento significativo da latência quando você acessa cada bloco de dados pela primeira vez em um novo volume do EBS que foi criado de um snapshot. É possível evitar essa ocorrência de performance usando uma das seguintes opções:

- Acessar cada bloco antes de colocar o volume em produção. Esse processo é chamado inicialização (conhecido anteriormente como pré-aquecimento). Para obter mais informações, consulte [Inicializar volumes de Amazon EBS \(p. 1463\)](#).
- Habilite as restauração rápida em um snapshot para garantir que os volumes do EBS criados de um snapshot sejam totalmente inicializados na criação e entreguem instantaneamente toda a sua performance provisionada. Para obter mais informações, consulte [Restauração rápida de snapshots do Amazon EBS \(p. 1434\)](#).

Fatores que podem reduzir a performance do HDD

Quando você cria um snapshot de um volume HDD otimizado para taxa de transferência (st1) ou HDD a frio (sc1), a performance poderá cair até o valor básico do volume enquanto o snapshot estiver em andamento. Esse comportamento é específico desses tipos de volumes. Outros fatores que podem limitar a performance incluem a orientação de uma taxa de transferência maior do que a instância pode oferecer suporte, a penalidade de performance encontrada ao inicializar volumes criados de um snapshot e as quantidades excessivas de pequenas operações de E/S aleatórias no volume. Para obter mais informações sobre como calcular a taxa de transferência para volumes de HDD, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#).

A performance também pode ser afetada se sua aplicação não estiver enviando solicitações de E/S suficientes. Isso pode ser monitorado verificando o comprimento da fila do volume e o tamanho da E/S. O comprimento da fila é o número de solicitações pendentes de E/S de sua aplicação para seu volume. Para obter máxima consistência, os volumes baseados em HDD devem manter um comprimento de fila (arredondado para o número inteiro mais próximo) de 4 ou mais ao executar E/S sequencial de 1 MiB. Para obter mais informações sobre como garantir a performance consistente de seus volumes, consulte [Características e monitoramento de E/S \(p. 1459\)](#)

Usar o RAID 0 para maximizar a utilização de recursos de instância

Alguns tipos de instância podem gerar taxas de transferência de E/S maiores do que o que você pode provisionar para um único volume do EBS. É possível adicionar vários volumes juntos em uma configuração de RAID 0 para usar a largura de banda disponível para essas instâncias. Para obter mais informações, consulte [Configuração RAID no Windows \(p. 1465\)](#).

Acompanhar a performance usando o Amazon CloudWatch

A Amazon Web Services fornece métricas de performance para o Amazon EBS que você pode analisar e exibir com o Amazon CloudWatch, e as verificações de status que você pode usar para monitorar a integridade de seus volumes. Para obter mais informações, consulte [Monitorar o status de seus volumes \(p. 1282\)](#).

Características e monitoramento de E/S

Em uma determinada configuração de volume, certas características de E/S controlam a performance dos volumes do EBS. Volumes baseados em SSD — SSD de uso geral (gp2 e gp3) e SSD de IOPS provisionadas (io1 e io2) — geram performance consistente quando uma operação de E/S é aleatória ou sequencial. Volumes baseados em HDD — HDD otimizado para taxa de transferência (st1) e HDD a frio (sc1) — geram performance ideal somente quando as operações de E/S são grandes e sequenciais. Para

entender como os volumes de SSD e HDD serão executados em sua aplicação, é importante saber sobre as conexões entre a demanda no volume, a quantidade de IOPS disponível para ele, o tempo necessário para que uma operação de E/S seja concluída e os limites de taxa de transferência do volume.

Tópicos

- [IOPS \(p. 1460\)](#)
- [Comprimento e latência da fila de volume \(p. 1461\)](#)
- [Limites de taxa de transferência de tamanho e volume de E/S \(p. 1461\)](#)
- [Monitorar as características de E/S usando o CloudWatch \(p. 1462\)](#)
- [Recursos relacionados \(p. 1462\)](#)

IOPS

IOPS é uma unidade de medida que representa operações de entrada/saída por segundo. As operações são medidas em KiB, e a tecnologia de disco subjacente determina a quantidade máxima de dados que um tipo de volume conta como uma única E/S. O tamanho de E/S é limitado a 256 KiB para volumes SSD e 1.024 KiB para volumes HDD porque os volumes SSD lidam com E/S pequena ou aleatória de forma muito mais eficiente do que os volumes HDD.

Quando operações de E/S pequenas são fisicamente sequenciais, o Amazon EBS tenta mesclá-las em uma única operação de E/S até o tamanho máximo de E/S. Da mesma maneira, quando operações de E/S são maiores do que o tamanho máximo de E/S, o Amazon EBS tenta dividí-las em operações de E/S menores. A tabela a seguir mostra alguns exemplos.

Tipo de volume	Tamanho máximo de E/S	Operações de E/S da sua aplicação	Número de IOPS	Observações
SSD	256 KiB	1 x operação de E/S de 1024 KiB	4 ($1.024 \div 256 = 4$)	O Amazon EBS divide a operação de E/S de 1.024 em quatro operações menores de 256 KiB.
		8 x operações de E/S sequenciais de 32 KiB	1 ($8 \times 32 = 256$)	O Amazon EBS mescla as oito operações sequenciais de E/S de 32 KiB em uma única operação de 256 KiB.
		8 operações de E/S aleatórias de 32 KiB	8	O Amazon EBS conta as operações de E/S aleatórias separadamente.
HDD	1.024 KiB	1 x operação de E/S de 1024 KiB	1	A operação de E/S já é igual ao tamanho máximo de E/S. Ela não é mesclada ou dividida.
		8 x operações de E/S sequenciais de 128 KiB	1 ($8 \times 128 = 1.024$)	O Amazon EBS mescla as oito operações sequenciais de E/S

Tipo de volume	Tamanho máximo de E/S	Operações de E/S da sua aplicação	Número de IOPS	Observações
				de 128 KiB em uma única operação de E/S de 1024 KiB.
		8 operações de E/S aleatórias de 32 KiB	8	O Amazon EBS conta as operações de E/S aleatórias separadamente.

Portanto, quando você cria um volume baseado em SSD com suporte a 3.000 IOPS (provisionando um volume de Provisioned IOPS SSD com 3.000 IOPS ou dimensionando um volume de Finalidade geral (SSD) com 1.000 GiB), e você o anexa a uma instância otimizada para EBS que pode fornecer largura de banda suficiente, você pode transferir até 3.000 E/S de dados por segundo, com a taxa de transferência determinada pelo tamanho de E/S.

Comprimento e latência da fila de volume

A fila de volume é o número de solicitações de E/S pendentes para um dispositivo. A latência é o tempo real, de ponta a ponta, do cliente para uma operação de E/S, ou seja, o tempo decorrido entre o envio de um E/S para o EBS e o recebimento de uma confirmação do EBS de que a leitura ou a gravação de E/S foram concluídas. O comprimento da fila deve ser adequadamente calibrado com o tamanho e a latência de E/S para evitar criar gargalos no sistema operacional convidado ou no link de rede para EBS.

O tamanho ideal da fila varia para cada workload, dependendo da sensibilidade de sua aplicação específica em relação à IOPS e à latência. Se sua workload não estiver fornecendo solicitações de E/S suficientes para usar integralmente a performance disponível para seu volume do EBS, o volume pode não fornecer a IOPS ou a taxa de transferência que você provisionou.

As aplicações com transações intensivas são sensíveis ao aumento de latência de E/S e são adequadas para volumes baseados em SSD. Você pode manter a IOPS alta e, ao mesmo tempo, a latência baixa mantendo uma fila de comprimento pequeno e um alto número de IOPS disponíveis para o volume. Se você gerar consistentemente mais IOPS para um volume do que ele dispõe, poderá causar o aumento da latência de E/S.

As aplicações com taxa de transferência intensiva são menos sensíveis ao aumento da latência de E/S e são bem adequadas para volumes baseados em HDD. Você pode manter alta taxa de transferência para volumes baseados em HDD mantendo uma fila de comprimento maior ao executar E/S grande e sequencial.

Limites de taxa de transferência de tamanho e volume de E/S

Para volumes baseados em SSD, se o tamanho de E/S for muito grande, você poderá ter um número menor de IOPS do que provisionou, porque você está chegando ao limite de taxa de transferência do volume. Por exemplo, um volume gp2 com menos de 1.000 GiB com créditos de intermitência disponíveis tem um limite de IOPS de 3.000 e um limite de volume de taxa de transferência de 250 MiB/s. Se você estiver usando um tamanho de E/S de 256 KiB, o volume atingirá o limite da taxa de transferência a 1000 IOPS ($1000 \times 256 \text{ KiB} = 250 \text{ MiB}$). Para E/S de tamanhos menores (por exemplo, 16 KiB), esse mesmo volume pode sustentar 3.000 IOPS porque a taxa de transferência está bem abaixo de 250 MiB/s. Estes exemplos supõem que a E/S do volume não atinge os limites de taxa de transferência da instância. Para obter mais informações sobre os limites de taxa de transferência para cada tipo de volume do EBS, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#).

Para operações menores de E/S, poderá surgir um valor de IOPS mais alto do que provisionado conforme medido dentro de sua instância. Isso acontece quando o sistema operacional da instância funde operações pequenas de E/S em uma operação maior antes de passá-las ao Amazon EBS.

Se sua workload usar E/S sequenciais em volumes `st1` e `sc1` baseados em HDD, você poderá ter um número de IOPS superior ao esperado conforme medido dentro de sua instância. Isso acontece quando o sistema operacional da instância funde operações de E/S sequenciais e as conta em unidades de 1.024 KiB. Se sua workload usar operações de E/S pequenas ou aleatórias, você poderá ter uma taxa de transferência menor do que o esperado. Isso porque nós contamos cada E/S aleatória, não sequencial, para a contagem total de IOPS, que podem levá-lo a atingir o limite de volume de IOPS mais cedo do que o esperado.

Seja qual for o tipo de volume do EBS, se a IOPS ou a taxa de transferência não forem conforme o esperado de acordo com a configuração, garanta que a largura de banda da instância do EC2 não seja o fator limitante. Você sempre deve usar uma instância otimizada para EBS da geração atual (ou uma que inclua a conectividade de rede 10 Gb/s) para a performance ideal. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#). Outra causa possível para a ausência da IOPS prevista é que você não está conduzindo E/S suficientes para volumes do EBS.

Monitorar as características de E/S usando o CloudWatch

Você pode monitorar essas características de E/S com as [métricas de volume do CloudWatch \(p. 1473\)](#) de cada volume. Métricas importantes a serem consideradas incluem o seguinte:

- `BurstBalance`
- `VolumeReadBytes`
- `VolumeWriteBytes`
- `VolumeReadOps`
- `VolumeWriteOps`
- `VolumeQueueLength`

`BurstBalance` exibe o saldo do bucket de intermitência para os volumes `gp2`, `st1` e `sc1` como um porcentual do saldo restante. Quando seu bucket de intermitência é esgotado, a E/S de volume (para volumes `gp2`) ou a taxa de transferência de volume (para volumes `st1` e `sc1`) são limitadas à linha de base. Verifique o valor `BurstBalance` para determinar se seu volume está sendo limitado por esse motivo. Para obter uma lista completa das métricas do Amazon EBS disponíveis, consulte [Métricas do Amazon EBS \(p. 1473\)](#) e [Métricas do Amazon EBS para instâncias baseadas em Nitro \(p. 906\)](#).

Os volumes `st1` e `sc1` baseados em HDD são projetados para ter performance melhor com workloads que aproveitam o tamanho de E/S máximo de 1.024 KiB. Para determinar o tamanho médio de E/S de seu volume, divida `VolumeWriteBytes` por `VolumeWriteOps`. O mesmo cálculo se aplica a operações de leitura. Se o tamanho de E/S médio ficar abaixo de 64 KiB, aumentando o tamanho de operações de E/S enviadas para um volume `st1` ou `sc1` o volume deve melhorar a performance.

Note

Se o tamanho médio de E/S for igual ou próximo de 44 KiB, você poderá usar uma instância ou um kernel sem suporte para descritores indiretos. Qualquer kernel do Linux versão 3.8 ou posterior tem esse suporte, bem como qualquer instância da geração atual.

Se a latência de E/S for maior de que você precisa, verifique `VolumeQueueLength` para se assegurar de que a aplicação não está tentando gerar mais IOPS do que você provisionou. Se a aplicação exigir um número maior de IOPS do que seu volume pode fornecer, será necessário considerar usar um volume de `gp2` maior com um nível de performance básica superior ou um volume de `io1` ou `io2` com mais IOPS provisionadas para atingir latências mais rápidas.

Recursos relacionados

Para obter mais informações sobre as características de E/S do Amazon EBS, consulte a seguinte apresentação re:Invent: [Amazon EBS: Como projetar visando a performance](#).

Inicializar volumes de Amazon EBS

Os volumes vazios do EBS recebem a performance máxima no momento em que são criados e não requerem inicialização (antes conhecida como pré-aquecimento).

Para volumes que foram criados de snapshots, os blocos de armazenamento devem ser extraídos do Amazon S3 e gravados no volume para poderem ser acessados. Essa ação preliminar leva tempo e pode causar um aumento significativo na latência de operações de E/S na primeira vez que cada bloco for acessado. A performance do volume é obtida depois que todos os blocos forem obtidos por download e gravados no volume.

Important

Durante a inicialização dos volumes de Provisioned IOPS SSD que foram criados de snapshots, a performance do volume pode ser reduzida para menos de 50% de seu nível esperado, o que faz com que o volume exiba um estado de `warning` na verificação do status de I/O Performance (Performance de E/S). Isso é esperado, e é possível ignorar o estado de `warning` em volumes de Provisioned IOPS SSD enquanto estiver inicializando esses volumes. Para obter mais informações, consulte [Verificações de status do volume do EBS \(p. 1282\)](#).

Para a maioria das aplicações, é aceitável a amortização do custo de inicialização ao longo da vida útil do volume. Para evitar essa ocorrência de performance inicial em um ambiente de produção, é possível usar uma das seguintes opções:

- Forçar a inicialização imediata do volume inteiro. Para obter mais informações, consulte [Inicializar volumes de Amazon EBS no Windows \(p. 1463\)](#).
- Habilite as restaurações rápidas em um snapshot para garantir que os volumes do EBS criados de um snapshot sejam totalmente inicializados na criação e entreguem instantaneamente toda a sua performance provisionada. Para obter mais informações, consulte [Restauração rápida de snapshots do Amazon EBS \(p. 1434\)](#).

Inicializar volumes de Amazon EBS no Windows

Os novos volumes do EBS recebem sua performance máxima no momento em que são disponibilizados e não requerem inicialização (antes conhecido como pré-aquecimento). Para volumes que foram criados de snapshots, use o dd ou o fio para que o Windows leia em todos os blocos em um volume. Todos os dados existentes no volume serão preservados.

Para obter informações sobre a inicialização de volumes do Amazon EBS no Linux, consulte [Inicializar volumes do Amazon EBS no Linux](#).

Antes de usar uma ou outra ferramenta, coleite informações sobre os discos no sistema como se segue:

Para reunir informações sobre os discos do sistema

1. Use o comando wmic para listar os discos disponíveis no sistema:

```
wmic diskdrive get size,deviceid
```

A seguir está um exemplo de saída:

DeviceID	Size
\\.\PHYSICALDRIVE2	80517265920
\\.\PHYSICALDRIVE1	80517265920
\\.\PHYSICALDRIVE0	128849011200
\\.\PHYSICALDRIVE3	107372805120

2. Identifique o disco para inicializar usando dd ou fio. A unidade C: está em \\.\PHYSICALDRIVE0. Você pode usar o utilitário diskmgmt.msc para comparar letras de unidades com números de unidades de disco, se não tiver certeza de que número de unidade usar.

Usar o dd

Conclua os seguintes procedimentos para instalar e usar dd para inicializar um volume.

Considerações importantes

- A inicialização do volume leva de vários minutos a várias horas, dependendo da largura de banda da instância do EC2, da IOPS provisionada para o volume e do tamanho do volume.
- O uso incorreto de dd pode destruir facilmente os dados de um volume. Certifique-se de seguir este procedimento com precisão.

Instalar dd para Windows

O programa dd para Windows fornece uma experiência semelhante ao programa dd que é geralmente disponível para sistemas Linux e Unix, e permite que você inicialize volumes do Amazon EBS que foram criados de snapshots. As versões beta mais recentes suportam o dispositivo /dev/null virtual. Se você instalar uma versão anterior, você pode usar o dispositivo nul virtual em vez disso. A documentação completa está disponível em <http://www.chrysocome.net/dd>.

1. Faça download da versão binária mais recente do dd para Windows em <http://www.chrysocome.net/dd>.
2. (Opcional) Crie uma pasta para utilitários de linha de comando que seja fácil de localizar e recordar, como C:\bin. Se você já tiver uma pasta designada para utilitários de linha de comando, poderá usar essa pasta na etapa a seguir.
3. Descompacte o pacote binário e copie o arquivo dd.exe para sua pasta de utilitários de linha de comando (por exemplo, C:\bin).
4. Adicione a pasta de utilitários de linha de comando à variável de ambiente de caminho para que você possa executar os programas nessa pasta de qualquer lugar.
 - a. Escolha Iniciar, abra o menu de contexto (clique com o botão direito) de Computador e escolha Propriedades.
 - b. Escolha Configurações avançadas de sistema, Variáveis de Ambiente.
 - c. Em Variáveis de Sistema, selecione a variável Caminho e escolha Editar.
 - d. Em Valor da variável, adicione um ponto e vírgula e o local de sua pasta de utilitário de linha de comando (;C:\bin\)) no final do valor existente.
 - e. Escolha OK para fechar a janela Editar Variável de Sistema.
5. Abra uma nova janela do prompt de comando. As seguintes etapas não atualizam as variáveis ambientais nas janelas de prompt de comando atuais. As janelas de prompt de comando que você abre agora que você concluiu a etapa anterior são atualizadas.

Inicializar um volume usando dd para Windows

Execute o seguinte comando para ler todos os blocos no dispositivo especificado (e envie a saída para o dispositivo virtual /dev/null). Este comando inicializa com segurança os dados existentes.

```
dd if=\\.\\PHYSICALDRIVEn of=/dev/null bs=1M --progress --size
```

Pode haver um erro se dd tentar ler além do fim do volume. Você pode ignorar isso com segurança.

Se você usou uma versão anterior do comando dd, ele não suporta o dispositivo /dev/null. Em vez disso, você pode usar o dispositivo nul da seguinte forma.

```
dd if=\\.\\PHYSICALDRIVEn of=nul bs=1M --progress --size
```

Usar o fio

Conclua os seguintes procedimentos para instalar e usar fio para inicializar um volume.

Como instalar fio para Windows

O programa fio para Windows fornece uma experiência semelhante ao programa fio que é geralmente disponível para sistemas Linux e Unix, e permite que você inicialize volumes do Amazon EBS criados de snapshots. Para obter mais informações, consulte <https://github.com/axboe/fio>.

1. Faça download do instalador do [fio MSI](#) (selecione a compilação x86 ou x64 mais recente e, depois, escolha Artifacts (Artefatos)).
2. Instalar o fio.

Como inicializar um volume usando fio para Windows

1. Executar um comando semelhante ao seguinte para inicializar um volume:

```
fio --filename=\\.\\PHYSICALDRIVEn --rw=read --bs=128k --iodepth=32 --direct=1 --  
name=volume-initialize
```

2. Quando a operação for concluída, você estará pronto para usar o novo volume. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#).

Configuração RAID no Windows

Com o Amazon EBS, você pode usar qualquer uma das configurações padrão RAID que você pode usar com um servidor bare metal tradicional, desde que essa configuração RAID específica tenha suporte no sistema operacional para sua instância. A razão disso é que todo o RAID é realizado no nível do software.

Os dados dos volumes do Amazon EBS são replicados em vários servidores em uma zona de disponibilidade para evitar perdas de dados causadas por falha em qualquer componente único. Essa replicação torna os volumes do Amazon EBS 10 vezes mais confiável do que as unidades de disco típicas. Para obter mais informações, consulte [Disponibilidade e durabilidade do Amazon EBS](#) nas páginas de detalhes do produto Amazon EBS.

Note

Você deve evitar inicializar a partir de um volume RAID. Se ocorre uma falha em um dos dispositivos, talvez você não consiga iniciar o sistema operacional.

Se você precisar criar uma matriz RAID em uma instância do Linux, consulte [Configuração de RAID no Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

- [Opções de configuração de RAID \(p. 1466\)](#)
- [Criar uma matriz RAID 0 no Windows \(p. 1466\)](#)
- [Criar snapshots de volumes em uma matriz RAID \(p. 1469\)](#)

Opcões de configuração de RAID

Criar uma matriz de RAID 0 permite atingir um nível de performance para um sistema de arquivos maior do que você pode provisionar em um único volume Amazon EBS. Use RAID 0 quando a performance de E/S for da máxima importância. Com o RAID 0, a E/S é distribuída entre os volumes em uma distribuição. Se você adicionar um volume, obterá a adição direta de taxa de transferência e IOPS. No entanto, lembre-se de que a performance da distribuição é limitada ao volume de pior performance do conjunto e que a perda de um único volume do conjunto resulta em perda de dados completa para a matriz.

O tamanho resultante de uma matriz de RAID 0 é a soma dos tamanhos dos volumes nela, e a largura de banda é a soma da largura de banda dos volumes nela. Por exemplo, dois volumes `io1` de 500 GiB, com 4.000 IOPS provisionadas cada, criarião uma matriz RAID 0 de 1.000 GiB com uma largura de banda disponível de 8.000 IOPS e 1.000 MiB/s de taxa de transferência.

Important

O RAID 5 e o RAID 6 não são recomendados para o Amazon EBS porque as operações de gravação de paridade desses modos de RAID consomem um pouco do IOPS disponível para os seus volumes. Dependendo da configuração de sua matriz de RAID, esses modos de RAID fornecem de 20 a 30% menos IOPS útil do que uma configuração de RAID 0. O maior custo também é um fator nesses modos de RAID; ao usar tamanhos e velocidades idênticos de volume, uma matriz de RAID 0 de 2 volumes pode superar uma matriz de RAID 6 de 4 volumes que custa duas vezes mais.

Também não se recomenda o uso do RAID 1 com o Amazon EBS. O RAID 1 exige mais largura de banda do Amazon EC2 para o Amazon EBS do que nas configurações sem RAID, pois os dados são gravados em vários volumes simultaneamente. Além disso, o RAID 1 não fornece nenhuma melhoria na performance de gravação.

Criar uma matriz RAID 0 no Windows

Esta documentação fornece um exemplo básico de configuração de RAID 0.

Antes de executar esse procedimento, você precisa decidir o tamanho que deve ter sua matriz de RAID 0 e quantos IOPS você deseja provisionar.

Use o procedimento a seguir para criar a matriz de RAID 0. Você pode obter instruções sobre instâncias do Linux em [Criar uma matriz RAID no Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Para criar uma matriz de RAID 0 no Windows

1. Crie os volumes do Amazon EBS para sua matriz. Para obter mais informações, consulte [Crie um volume do Amazon EBS. \(p. 1268\)](#).

Important

Crie volumes com valores de performance de IOPS e tamanho idênticos para sua matriz. Certifique-se de não criar uma matriz que exceda a largura de banda disponível de sua instância do EC2.

2. Anexe os volumes do Amazon EBS à instância na qual você deseja hospedar a matriz. Para obter mais informações, consulte [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#).
3. Conecte-se à sua instância do Windows. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
4. Abra um prompt de comando e digite o comando `diskpart`.

```
diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
```

On computer: WIN-BM6QPPL51CO

5. No prompt DISKPART, liste os discos disponíveis com o seguinte comando.

```
DISKPART> list disk

Disk ###  Status     Size      Free      Dyn  Gpt
-----  -----
Disk 0    Online     30 GB    0 B
Disk 1    Online     8 GB     0 B
Disk 2    Online     8 GB     0 B
```

Identifique os discos que deseja usar em sua matriz e anote os números dos discos.

6. Cada disco que deseja usar em sua matriz deve ser um disco dinâmico online que não contenha nenhum volume existente. Use as seguintes etapas para converter discos básicos em discos dinâmicos e excluir todos os volumes existentes.

- a. Selecione um disco que deseja usar em sua matriz com o seguinte comando, substituindo **n** pelo número do disco.

```
DISKPART> select disk n

Disk n is now the selected disk.
```

- b. Se o disco selecionado estiver listado como **Offline**, ative-o executando o comando **online disk**.
c. Se o disco selecionado não tiver um asterisco na coluna **Dyn** na saída do comando **list disk** anterior, você precisará convertê-lo em um disco dinâmico.

```
DISKPART> convert dynamic
```

Note

Se você receber um erro de que o disco é protegido contra gravação, desmarque o sinalizador de somente leitura no comando **ATTRIBUTE DISK CLEAR READONLY** e tente novamente a conversão do disco dinâmico.

- d. Use o comando **detail disk** para verificar se há volumes existentes no disco selecionado.

```
DISKPART> detail disk

XENSRV PVDISK SCSI Disk Device
Disk ID: 2D8BF659
Type   : SCSI
Status  : Online
Path   : 0
Target  : 1
LUN ID : 0
Location Path : PCIROOT(0)#PCI(0300)#SCSI(P00T01L00)
Current Read-only State : No
Read-only : No
Boot Disk : No
Pagefile Disk : No
Hibernation File Disk : No
Crashdump Disk : No
Clustered Disk : No

Volume ###  Ltr  Label        Fs      Type       Size    Status     Info
-----  ---  ---  -----
Volume 2      D   NEW VOLUME  FAT32   Simple    8189 MB  Healthy
```

Anote todos os números de volumes no disco. Neste exemplo, o número do volume é 2. Se não houver volumes, ignore a próxima etapa.

- e. (Necessário somente se foram encontrados volumes na etapa anterior) Selecione e exclua todos os volumes existentes no disco que você identificou na etapa anterior.

Warning

Isso destrói todos os dados existentes no volume.

- i. Selecione o volume, substituindo **n** pelo número do volume.

```
DISKPART> select volume n
Volume n is the selected volume.
```

- ii. Exclua o volume.

```
DISKPART> delete volume

DiskPart successfully deleted the volume.
```

- iii. Repita essas subetapas para cada volume que você precisa excluir no disco selecionado.

- f. Repita [Step 6 \(p. 1467\)](#) para cada disco que deseja usar em sua matriz.

7. Verifique se os discos que você deseja usar agora são dinâmicos. Nesse caso, estamos usando discos 1 e 2 para o volume RAID.

```
DISKPART> list disk

Disk ### Status Size Free Dyn Gpt
----- -----
Disk 0 Online 30 GB 0 B
Disk 1 Online 8 GB 0 B *
Disk 2 Online 8 GB 0 B *
```

8. Crie a matriz de RAID. No Windows, um volume de RAID 0 é referido como um volume distribuído.

Para criar uma matriz de volume distribuído nos discos 1 e 2, use o seguinte comando (observe a opção **stripe** para distribuir a matriz):

```
DISKPART> create volume stripe disk=1,2
DiskPart successfully created the volume.
```

9. Verifique seu novo volume.

```
DISKPART> list volume

DISKPART> list volume

Volume ### Ltr Label Fs Type Size Status Info
----- -- -- --
Volume 0 C NTFS Partition 29 GB Healthy System
Volume 1 RAW Stripe 15 GB Healthy
```

Observe que a coluna **Type** agora indica que o Volume 1 é um volume **stripe**.

10. Selecione e formate seu volume para que você possa começar a usá-lo.

- a. Selecione o volume que você deseja formatar, substituindo **n** pelo número do volume.

```
DISKPART> select volume n  
  
Volume n is the selected volume.
```

- b. Formate o volume.

Note

Para executar uma formatação completa, omita a opção quick.

```
DISKPART> format quick recommended label="My new volume"  
  
100 percent completed  
  
DiskPart successfully formatted the volume.
```

- c. Atribua uma letra de unidade disponível ao seu volume.

```
DISKPART> assign letter f  
  
DiskPart successfully assigned the drive letter or mount point.
```

Seu novo volume agora está pronto para uso.

Criar snapshots de volumes em uma matriz RAID

Se você deseja fazer backup dos dados nos volumes do EBS em um array RAID usando snapshots, você deve verificar se os snapshots estão consistentes. Isso ocorre porque os snapshots desses volumes são criados de maneira independente. Restaurar os volumes do EBS em uma matriz RAID de snapshots que não estão sincronizados prejudicaria a integridade da matriz.

Para criar um conjunto consistente de snapshots para a matriz RAID, use [snapshots de vários volumes do EBS](#). Com os snapshots de vários volumes, é possível tirar snapshots de momentos específicos, coordenados por dados e consistentes com falhas em vários volumes do EBS associados a uma instância do EC2. Não é necessário interromper a instância para coordenar entre volumes a fim de garantir consistência, pois os snapshots são tirados automaticamente em vários volumes do EBS. Para obter mais informações, consulte as etapas para criar snapshots de vários volumes em [Criar snapshots do Amazon EBS](#).

Comparar volumes do EBS

Você pode testar a performance dos volumes do Amazon EBS simulando workloads de E/S. O processo é o seguinte:

1. Execute uma instância otimizada para EBS.
2. Crie novos volumes do EBS.
3. Anexe os volumes à sua instância otimizada para EBS.
4. Configure e monte o dispositivo de blocos.
5. Instale uma ferramenta para comparar a performance de E/S.
6. Compare a performance de E/S de seus volumes.
7. Exclua os volumes e encerre sua instância para não continuar a ser cobrado.

Important

Alguns procedimentos resultam na destruição de dados existentes em volumes do EBS que você compara. Os procedimentos de comparação são destinados ao uso em volumes criados especialmente para fins de teste, não volumes de produção.

Configurar a instância

Para obter a performance ideal em volumes do EBS, recomendamos que você use uma instância otimizada para EBS. As instâncias otimizadas para EBS fornecem taxa de transferência dedicada entre o Amazon EC2 e o Amazon EBS, com instância. As instâncias otimizadas para EBS fornecem largura de banda dedicada entre o Amazon EC2 e o Amazon EBS, com especificações que dependem do tipo de instância. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

Para criar uma instância otimizada para EBS, escolha Launch as an EBS-Optimized instance ao executar a instância usando o console do Amazon EC2 ou especifique --ebs-optimized ao utilizar a linha de comando. Certifique-se de executar uma instância de geração atual que ofereça suporte a essa opção. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#).

Configurar volumes de Provisioned IOPS SSD ou Finalidade geral (SSD)

Para criar volumes SSD de IOPS provisionadas (io1 e io2) ou SSD de uso geral (gp2 e gp3) usando o console do Amazon EC2, em Volume type (Tipo de volume), escolha Provisioned IOPS SSD (io1) (SSD de IOPS provisionadas (io1)), Provisioned IOPS SSD (io2) (SSD de IOPS provisionadas (io2)), General Purpose SSD (gp2) (SSD de uso geral (gp2)) ou General Purpose SSD (gp3) (SSD de uso geral (gp3)). Na linha de comando, especifique io1, io2, gp2 ou gp3 para o parâmetro --volume-type. Para os volumes de io1, io2, e gp3, especifique o número de operações de E/S por segundo (IOPS) para o parâmetro --iops. Para obter mais informações, consulte [Tipos de volume do Amazon EBS \(p. 1247\)](#) e [Crie um volume do Amazon EBS. \(p. 1268\)](#).

Configurar volumes HDD otimizado para taxa de transferência (st1) ou HDD a frio (sc1)

Para criar um volume st1, escolha Throughput Optimized HDD (HDD otimizado para taxa de transferência) ao criar o volume usando o console do Amazon EC2 ou especifique --type st1 ao usar a linha de comando. Para criar um volume sc1, escolha Cold HDD (HDD a frio) ao criar o volume usando o console do Amazon EC2 ou especifique --type sc1 ao usar a linha de comando. Para obter informações sobre a criação de volumes do EBS, consulte [Crie um volume do Amazon EBS. \(p. 1268\)](#). Para obter informações sobre como anexar esses volumes à sua instância, consulte [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#).

Instalar ferramentas de comparação

A tabela a seguir lista algumas ferramentas possíveis que você pode usar para comparar a performance dos volumes do EBS.

Ferramenta	Descrição
DiskSpd	O DiskSpd é uma ferramenta de performance de armazenamento das equipes de engenharia do Windows, Windows Server e Cloud Server Infrastructure na Microsoft. Disponível para download em https://github.com/Microsoft/diskspd/releases . Depois de fazer download do arquivo executável <code>diskspd.exe</code> , abra um prompt de comando com direitos administrativos (escolhendo “Executar como administrador”) e navegue até o diretório onde você copiou o arquivo <code>diskspd.exe</code> . Copie o arquivo executável <code>diskspd.exe</code> desejado da pasta executável apropriada, <code>amd64fre</code> , <code>armfre</code> ou <code>x86fre</code>) para um caminho curto e simples,

Ferramenta	Descrição
	como C:\DiskSpd. Na maioria dos casos, você desejará a versão de 64 bits do DiskSpd da pasta amd64fre. O código-fonte do DiskSpd está hospedado no GitHub em: https://github.com/Microsoft/diskspd .
CrystalDiskMark	CrystalDiskMark é um software de benchmark de disco simples. Ele está disponível para download em https://crystalmark.info/en/software/crystaldiskmark/ .

Essas ferramentas de avaliação oferecem suporte a uma ampla variedade de parâmetros de teste. Você deve usar os comandos que aproximam workloads às quais seus volumes oferecerão suporte. Os comandos fornecidos abaixo servem como exemplos para ajudá-lo a começar a usar.

Escolha o comprimento da fila de volume

Escolha do melhor comprimento da fila de volume com base em sua workload e tipo de volume.

Tamanho da fila em volumes baseados em SSD

Para determinar o tamanho ideal da fila para sua workload em volumes baseados em SSD, recomendamos focar em um tamanho da fila de 1 para cada 1.000 IOPS disponíveis (linha de base para volumes de Finalidade geral (SSD) e a quantidade provisionada para volumes de Provisioned IOPS SSD). Depois, você pode monitorar a performance de sua aplicação e ajustar esse valor com base nos requisitos da aplicação.

Aumentar o comprimento da fila é benéfico até que você atinja as IOPS provisionadas, a taxa de transferência ou o valor ideal de comprimento da fila de sistema, que é atualmente configurado como 32. Por exemplo, para um volume com 3.000 IOPS provisionadas deve-se ter como meta um comprimento de fila 3. Você deve experimentar ajustar esses valores para cima ou para baixo para ver qual funciona melhor para sua aplicação.

Tamanho da fila em volumes baseados em HDD

Para determinar o tamanho ideal da fila para sua workload em volumes baseados em HDD, recomendamos que você foque em um comprimento da fila pelo menos 4 ao executar operações de E/S sequenciais de 1 MiB. Depois, você pode monitorar a performance de seu aplicativo e ajustar esse valor com base nos requisitos do aplicativo. Por exemplo, um volume st1 de 2 TiB com taxa de transferência de intermitência de 500 MiB/s e IOPS de 500 deve focar em um comprimento da fila de 4, 8 ou de 16 ao executar operações de E/S sequenciais de 1.024 KiB, 512 KiB ou 256 KiB respectivamente. Você deve experimentar ajustar esses valores para cima ou para baixo e ver qual funciona melhor com sua aplicação.

Desabilitar estados C

Antes de executar a referência, desative os estados C do processador. Desativar os núcleos temporariamente em uma CPU compatível pode entrar em um estado C para economizar energia. Quando o núcleo é chamado para retomar o processamento, leva um determinado tempo até o núcleo voltar a funcionar por completo. Esta latência pode interferir nas rotinas de comparação do processador. Para obter mais informações sobre estados C e quais tipos de instância do EC2 são compatíveis a eles, consulte [Controle de estado do processador para sua instância do EC2](#).

Desativar estados C no Windows

Você pode desativar os estados C no Windows da seguinte maneira:

1. No PowerShell, obtenha o esquema de energia ativo atual.

```
$current_scheme = powercfg /getactivescheme
```

2. Obtenha o GUID do esquema de energia.

```
(Get-WmiObject -class Win32_PowerPlan -Namespace "root\cimv2\power" -Filter "ElementName='High performance'").InstanceID
```

3. Obtenha o GUID da configuração de energia.

```
(Get-WmiObject -class Win32_PowerSetting -Namespace "root\cimv2\power" -Filter "ElementName='Processor idle disable'").InstanceID
```

4. Obtenha o GUID do subgrupo da configuração de energia.

```
(Get-WmiObject -class Win32_PowerSettingSubgroup -Namespace "root\cimv2\power" -Filter "ElementName='Processor power management'").InstanceID
```

5. Desative os estados C definindo o valor do índice como 1. Um valor igual a 0 indica que os estados C estão desativados.

```
powercfg /  
setacvalueindex <power_scheme_guid> <power_setting_subgroup_guid> <power_setting_guid>  
1
```

6. Defina o esquema ativo para garantir que as configurações sejam salvas.

```
powercfg /setactive <power_scheme_guid>
```

Benchmarking de performance

Os seguintes procedimentos descrevem comandos de comparação para vários tipos de volumes do EBS.

Execute os seguintes comandos em uma instância otimizada para EBS com volumes do EBS anexados. Se os volumes do EBS tiverem sido criados de snapshots, initialize-os antes do benchmarking. Para obter mais informações, consulte [Iniciar volumes de Amazon EBS \(p. 1463\)](#).

Quando você terminar de testar seus volumes, consulte os seguintes tópicos para obter ajuda para limpar: [Excluir um volume de Amazon EBS \(p. 1293\)](#) e [Encerrar a instância \(p. 474\)](#).

Avalie a performance dos volumes de Provisioned IOPS SSD e Finalidade geral (SSD)

Execute DiskSpd no volume que você criou.

O comando a seguir executará um teste de E/S aleatório de 30 segundos usando um arquivo de teste de 20 GB localizado na unidade C:, com taxas de 25% de gravação e de 75% de leitura e um tamanho de bloco de 8 K. Ele usará oito threads de operador, cada um com quatro operações de E/S pendentes, e uma semente de valor de entropia de gravação de 1 GB. Os resultados do teste serão salvos em um arquivo de texto chamado DiskSpeedResults.txt. Esses parâmetros simulam uma workload OLTP do SQL Server.

```
diskspd -b8K -d30 -o4 -t8 -h -r -w25 -L -Z1G -c20G C:\iotest.dat > DiskSpeedResults.txt
```

Para obter mais informações sobre como interpretar os resultados, consulte este tutorial: [Inspeccionar a performance de E/S com o DiskSPD](#).

Métricas do Amazon CloudWatch para o Amazon EBS

As métricas do Amazon CloudWatch são dados estatísticos que você pode usar para visualizar, analisar e definir alarmes sobre o comportamento operacional de seus volumes.

Os dados são disponibilizados automaticamente em períodos de um minuto, sem custo adicional.

Quando obtém dados do CloudWatch, você pode incluir um parâmetro de solicitação `Period` para especificar a granularidade dos dados retornados. Esse período é diferente do que usamos quando coletamos os dados (períodos de um minuto). Recomendamos que você especifique em sua solicitação um período que seja igual ou maior do que o período de coleta para garantir que os dados retornados sejam válidos.

Você pode obter os dados usando a API do CloudWatch ou o console do Amazon EC2. O console usa os dados brutos da API do CloudWatch e exibe uma série de gráficos com base nos dados. Dependendo de suas necessidades, você pode preferir usar os dados da API ou os gráficos no console.

Tópicos

- [Métricas do Amazon EBS \(p. 1473\)](#)
- [Dimensões para métricas do Amazon EBS \(p. 1478\)](#)
- [Gráficos no console do Amazon EC2 \(p. 1478\)](#)

Métricas do Amazon EBS

O Amazon Elastic Block Store (Amazon EBS) envia pontos de dados para o CloudWatch para várias métricas. Todos os tipos de volume do Amazon EBS enviam automaticamente métricas de 1 minuto para o CloudWatch, mas somente quando o volume está anexado a uma instância.

Métricas

- [Métricas de volume para volumes anexados a todos os tipos de instância \(p. 1473\)](#)
- [Métricas de volume para volumes anexados a tipos de instância baseadas em Nitro \(p. 1477\)](#)
- [Métricas de restauração rápida do snapshot \(p. 1477\)](#)

Métricas de volume para volumes anexados a todos os tipos de instância

O namespace `AWS/EBS` inclui as métricas a seguir para volumes do EBS que estão anexados a todos os tipos de instância. Para obter informações sobre o espaço em disco disponível do sistema operacional em uma instância, consulte [Visualizar espaço livre em disco \(p. 1277\)](#).

Note

- Algumas métricas têm diferenças em instâncias criadas no sistema Nitro. Para obter uma lista desses tipos de instância, consulte [Instâncias criadas no Sistema Nitro \(p. 154\)](#).
- O namespace `AWS/EC2` inclui métricas adicionais do Amazon EBS para os volumes anexados a instâncias baseadas em Nitro que não são instâncias bare metal. Para obter mais informações sobre essas métricas, consulte [Métricas do Amazon EBS para instâncias baseadas em Nitro \(p. 906\)](#).

Métrica	Descrição
<code>VolumeReadBytes</code>	Fornece informações sobre as operações de leitura em um período especificado. A estatística <code>Sum</code> reporta o número total de bytes transferidos durante o período. A estatística <code>Average</code> informa o tamanho médio de cada operação de leitura durante o período, exceto em volumes anexados a uma instância baseada em Nitro, em que a média se refere a um período especificado. A estatística <code>SampleCount</code> informa o número total de operações de leitura durante o período, exceto nos volumes anexados a uma instância baseada em Nitro, em que a contagem de amostras

Métrica	Descrição
	<p>representa o número de pontos de dados utilizados no cálculo estatístico. Para instâncias de Xen, os dados são informados apenas quando há atividades de leitura no volume.</p> <p>As estatísticas Minimum e Maximum nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidades: bytes</p>
VolumeWriteBytes	<p>Fornece informações sobre as operações de gravação em um período especificado. A estatística Sum reporta o número total de bytes transferidos durante o período. A estatística Average informa o tamanho médio de cada operação de gravação durante o período, exceto em volumes anexados a uma instância baseada em Nitro, em que a média se refere a um período especificado. A estatística SampleCount informa o número total de operações de gravação durante o período, exceto nos volumes anexados a uma instância baseada em Nitro, em que a contagem de amostras representa o número de pontos de dados utilizados no cálculo estatístico. Para instâncias de Xen, os dados são informados apenas quando há atividades de gravação no volume.</p> <p>As estatísticas Minimum e Maximum nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidades: bytes</p>
VolumeReadOps	<p>O número total de operações de leitura em um período especificado. Observação: as operações de leitura são contadas após a conclusão.</p> <p>Para calcular a média de operações de leitura por segundo (IOPS de leitura) para o período, divida o total das operações de leitura pelo número de segundos no período em questão.</p> <p>As estatísticas Minimum e Maximum nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidades: contagem</p>
VolumeWriteOps	<p>O número total de operações de gravação em um período especificado. Observação: as operações de gravação são contadas após a conclusão.</p> <p>Para calcular a média de operações de gravação por segundo (IOPS de gravação) para o período, divida o total das operações de gravação pelo número de segundos no período em questão.</p> <p>As estatísticas Minimum e Maximum nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidades: contagem</p>

Métrica	Descrição
<code>VolumeTotalReadTime</code>	<p>Note</p> <p>Essa métrica não é compatível com volumes ativados Multi-Attach.</p> <p>O número total de segundos gastos por todas as operações de leitura que foram concluídas em um período especificado. Se várias solicitações são enviadas ao mesmo tempo, esse total pode ser maior do que a duração do período. Por exemplo, para um período de 1 minuto (60 segundos): se 150 operações foram concluídas durante esse período, e cada operação levou 1 segundo, o valor seria 150 segundos. Para instâncias de Xen, os dados são informados apenas quando há atividades de leitura no volume.</p> <p>A estatística <code>Average</code> nessa métrica não é relevante para volumes anexados a instâncias baseadas em Nitro.</p> <p>As estatísticas <code>Minimum</code> e <code>Maximum</code> nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidade: segundos</p>
<code>VolumeTotalWriteTime</code>	<p>Note</p> <p>Essa métrica não é compatível com volumes ativados Multi-Attach.</p> <p>O número total de segundos gastos por todas as operações de gravação que foram concluídas em um período especificado. Se várias solicitações são enviadas ao mesmo tempo, esse total pode ser maior do que a duração do período. Por exemplo, para um período de 1 minuto (60 segundos): se 150 operações foram concluídas durante esse período, e cada operação levou 1 segundo, o valor seria 150 segundos. Para instâncias de Xen, os dados são informados apenas quando há atividades de gravação no volume.</p> <p>A estatística <code>Average</code> nessa métrica não é relevante para volumes anexados a instâncias baseadas em Nitro.</p> <p>As estatísticas <code>Minimum</code> e <code>Maximum</code> nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidade: segundos</p>

Métrica	Descrição
VolumeIdleTime	<p>Note</p> <p>Essa métrica não é compatível com volumes ativados Multi-Attach.</p> <p>O número total de segundos em um período de tempo especificado quando nenhuma operação de leitura ou de gravação foi enviada.</p> <p>A estatística Average nessa métrica não é relevante para volumes anexados a instâncias baseadas em Nitro.</p> <p>As estatísticas Minimum e Maximum nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidade: segundos</p>
VolumeQueueLength	<p>O número de solicitações de operação de leitura e gravação aguardando conclusão em um período de tempo especificado.</p> <p>A estatística Sum nessa métrica não é relevante para volumes anexados a instâncias baseadas em Nitro.</p> <p>As estatísticas Minimum e Maximum nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidades: contagem</p>
VolumeThroughputPercentage	<p>Note</p> <p>Essa métrica não é compatível com volumes ativados Multi-Attach.</p> <p>Usado somente com volumes do Provisioned IOPS SSD. A porcentagem de operações de E/S por segundo (IOPS) entregues do total de IOPS provisionadas para um volume do Amazon EBS. Os volumes SSD de IOPS provisionadas fornecem a performance provisionada em 99,9% do tempo.</p> <p>Durante uma gravação, se não há outras solicitações pendentes de I/O em um minuto, o valor da métrica será 100%. Além disso, a performance de E/S de um volume pode se degradar temporariamente devido a uma ação que você tenha realizado (por exemplo, criar um snapshot de um volume durante o uso máximo, executar o volume em uma instância não otimizada para EBS ou acessar dados no volume pela primeira vez).</p> <p>Unidades: percentual</p>

Métrica	Descrição
VolumeConsumedReadWriteOps	<p>Usado somente com volumes do Provisioned IOPS SSD. A quantidade total de operações de leitura e gravação (normalizada para unidades de capacidade de 256 K) consumida em um período de tempo especificado.</p> <p>As operações de I/O menores que 256 K contam como 1 IOPS consumida. Operações de I/O maiores que 256 K são contadas em unidades de capacidade de 256 K. Por exemplo, uma I/O de 1.024 K seria computada como 4 IOPS consumidas.</p> <p>Unidades: contagem</p>
BurstBalance	<p>Usado somente com volumes SSD de uso geral (gp2), HDD otimizado para taxa de transferência (st1) e HDD a frio (sc1). Fornece informações sobre a porcentagem de créditos de E/S (para gp2) ou de créditos de taxa de transferência (para st1 e sc1) restante no bucket de intermitência. Os dados são reportados para o CloudWatch somente quando o volume está ativo. Se o volume não está conectado, nenhum dado é relatado.</p> <p>A estatística <code>Sum</code> dessa métrica não é relevante para volumes anexados a instâncias criadas no sistema Nitro.</p> <p>Se a performance basal do volume exceder a performance de intermitência máxima, os créditos nunca serão gastos. Se o volume estiver anexado a uma instância criada no Sistema Nitro, o equilíbrio de intermitência não será relatado. Para outras instâncias, o equilíbrio de intermitência relatado é de 100%. Para obter mais informações, consulte Créditos de E/S e performance de intermitência (p. 1251).</p> <p>Unidades: percentual</p>

Métricas de volume para volumes anexados a tipos de instância baseadas em Nitro

O namespace AWS/EC2 inclui métricas adicionais do Amazon EBS para os volumes anexados a instâncias baseadas em Nitro que não são instâncias bare metal. Para obter mais informações sobre essas métricas, consulte, [Métricas do Amazon EBS para instâncias baseadas em Nitro \(p. 906\)](#).

Métricas de restauração rápida do snapshot

O namespace AWS/EBS inclui as métricas a seguir para [restauração rápida de snapshots \(p. 1434\)](#).

Métrica	Descrição
FastSnapshotRestoreCreditsBucket	<p>O limite máximo do volume cria créditos que podem ser acumulados. Essa métrica é informada por snapshot e por zona de disponibilidade.</p> <p>A estatística mais significativa é <code>Average</code>. Os resultados das estatísticas de <code>Minimum</code> e <code>Maximum</code> são iguais aos de <code>Average</code> e podem ser usados no lugar.</p>

Métrica	Descrição
<code>FastSnapshotRestoreCreditsBalance</code>	<p>Este é o número de volume que cria créditos disponíveis. Essa métrica é informada por snapshot e por zona de disponibilidade.</p> <p>A estatística mais significativa é <code>Average</code>. Os resultados das estatísticas de <code>Minimum</code> e <code>Maximum</code> são iguais aos de <code>Average</code> e podem ser usados no lugar.</p>

Dimensões para métricas do Amazon EBS

A dimensão compatível é o ID do volume (`VolumeId`). Todas as estatísticas disponíveis são filtradas por ID do volume.

Para as [métricas de volume \(p. 1473\)](#), a dimensão compatível é o ID do volume (`VolumeId`). Todas as estatísticas disponíveis são filtradas por ID do volume.

Para as [métricas de restauração rápida de snapshots \(p. 1477\)](#), as dimensões compatíveis são ID do snapshot (`SnapshotId`) e zona de disponibilidade (`AvailabilityZone`).

Gráficos no console do Amazon EC2

Depois de criar um volume, você visualizará os gráficos de monitoramento de volumes no console do Amazon EC2. Selecione um volume na página Volumes no console e escolha Monitoring. A tabela a seguir lista os gráficos exibidos. A coluna à direita descreve como as métricas de dados brutos da API do CloudWatch são usadas para produzir cada gráfico. O período de todos os gráficos é de cinco minutos.

Gráfico	Descrição usando métricas brutas
Largura de banda de leitura (KiB/s)	<code>Sum(VolumeReadBytes) / Period / 1024</code>
Largura de banda de gravação (KiB/s)	<code>Sum(VolumeWriteBytes) / Period / 1024</code>
Taxa de transferência de leitura (IOPS)	<code>Sum(VolumeReadOps) / Period</code>
Taxa de transferência de gravação (IOPS)	<code>Sum(VolumeWriteOps) / Period</code>
Comprimento médio da fila (operações)	<code>Avg(VolumeQueueLength)</code>
% de tempo ocioso gasto	<code>Sum(VolumeIdleTime) / Period × 100</code>
Tamanho médio de leitura (KiB/operação)	<p><code>Avg(VolumeReadBytes) / 1024</code></p> <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera o tamanho médio de leitura usando a Matemática de métricas do CloudWatch:</p> $(\text{Sum}(\text{VolumeReadBytes}) / \text{Sum}(\text{VolumeReadOps})) / 1024$ <p>As métricas <code>VolumeReadBytes</code> e <code>VolumeReadOps</code> estão disponíveis no console do EBS CloudWatch.</p>

Gráfico	Descrição usando métricas brutas
Tamanho médio de gravação (KiB/ operação)	<p>Avg(VolumeWriteBytes) / 1024</p> <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera o tamanho médio de gravação usando a Matemática de métricas do CloudWatch:</p> $(\text{Sum}(VolumeWriteBytes) / \text{Sum}(VolumeWriteOps)) / 1024$ <p>As métricas VolumeWriteBytes e VolumeWriteOps estão disponíveis no console do EBS CloudWatch.</p>
Latência média de leitura (ms/ operação)	<p>Avg(VolumeTotalReadTime) × 1000</p> <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera a latência média de leitura usando a Matemática de métricas do CloudWatch:</p> $(\text{Sum}(VolumeTotalReadTime) / \text{Sum}(VolumeReadOps)) \times 1000$ <p>As métricas VolumeTotalReadTime e VolumeReadOps estão disponíveis no console do EBS CloudWatch.</p>
Latência média de gravação (ms/ operação)	<p>Avg(VolumeTotalWriteTime) × 1000</p> <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera a latência média de gravação usando a Matemática de métricas do CloudWatch:</p> $(\text{Sum}(VolumeTotalWriteTime) / \text{Sum}(VolumeWriteOps)) * 1000$ <p>As métricas VolumeTotalWriteTime e VolumeWriteOps estão disponíveis no console do EBS CloudWatch.</p>

Para os gráficos de latência média e os gráficos de tamanho médio, a média é calculada em relação ao número total de operações (leitura ou gravação, a que for aplicável ao gráfico) concluídas durante o período.

Amazon CloudWatch Events para Amazon EBS

O Amazon EBS emite notificações com base no Amazon CloudWatch Events para uma variedade de alterações no status da criptografia, do snapshot e do volume. Com o CloudWatch Events, você pode estabelecer regras que acionam ações programáticas em resposta a uma alteração no estado da chave de criptografia, do snapshot ou do volume. Por exemplo, quando um snapshot é criado, você pode acionar uma função do AWS Lambda para compartilhar o snapshot concluído com outra conta ou copiá-lo em outra região para fins de recuperação de desastres.

Os eventos no CloudWatch são representados como objetos JSON. Os campos que são exclusivos do evento estão contidos na seção "detalhes" do objeto JSON. O campo "evento" contém o nome do evento. O campo "resultados" contém o status concluído da ação que acionou o evento. Para obter mais informações, consulte [Padrões de eventos no CloudWatch Events](#) no Manual do usuário do Amazon CloudWatch Events.

Para obter mais informações, consulte [Como usar eventos](#) no Guia do usuário do Amazon CloudWatch.

Tópicos

- [Eventos de volume do EBS \(p. 1480\)](#)
- [Eventos de snapshot do EBS \(p. 1483\)](#)
- [Eventos de modificação de volume do EBS \(p. 1486\)](#)
- [Eventos de restauração rápida do snapshot do EBS \(p. 1487\)](#)
- [Usar o AWS Lambda para lidar com o CloudWatch Events \(p. 1488\)](#)

Eventos de volume do EBS

O Amazon EBS envia eventos para o CloudWatch Events quando ocorrem os eventos de volume a seguir.

Eventos

- [Criar volume \(createVolume\) \(p. 1480\)](#)
- [Excluir volume \(deleteVolume\) \(p. 1481\)](#)
- [Anexar ou reanexar volumes \(attachVolume, reattachVolume\) \(p. 1482\)](#)

Criar volume (createVolume)

O evento `createVolume` é enviado à sua conta da AWS quando uma ação para criar um volume for concluída. Contudo, não é salvo, registrado ou arquivado. Esse evento pode ter um resultado de `available` ou `failed`. Ocorrerá uma falha se uma AWS KMS key inválida for fornecida, conforme mostrado nos exemplos abaixo.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS para um evento `createVolume` bem-sucedido.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Volume Notification",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"  
    ],  
    "detail": {  
        "result": "available",  
        "cause": "",  
        "event": "createVolume",  
        "request-id": "01234567-0123-0123-0123-0123456789ab"  
    }  
}
```

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `createVolume` com falha. A causa da falha foi uma Chave do KMS desabilitada.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-0123456789ab",  
    "detail-type": "EBS Volume Notification",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"  
    ],  
    "detail": {  
        "result": "failed",  
        "cause": "KMS key not found or disabled",  
        "event": "createVolume",  
        "request-id": "01234567-0123-0123-0123-0123456789ab"  
    }  
}
```

```
"source": "aws.ec2",
"account": "012345678901",
"time": "yyyy-mm-ddThh:mm:ssZ",
"region": "sa-east-1",
"resources": [
    "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
],
"detail": {
    "event": "createVolume",
    "result": "failed",
    "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is disabled.",
    "request-id": "01234567-0123-0123-0123-0123456789ab",
}
}
```

A lista a seguir é um exemplo de um objeto JSON emitido por EBS depois de um evento `createVolume` com falha. A causa da falha foi a importação pendente de uma Chave do KMS.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "EBS Volume Notification",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "sa-east-1",
    "resources": [
        "arn:aws:ec2:sa-east-1:0123456789ab:volume/vol-01234567",
    ],
    "detail": {
        "event": "createVolume",
        "result": "failed",
        "cause": "arn:aws:kms:sa-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending import.",
        "request-id": "01234567-0123-0123-0123-0123456789ab",
    }
}
```

Excluir volume (deleteVolume)

O evento `deleteVolume` é enviado à sua conta da AWS quando uma ação para excluir um volume for concluída. Contudo, não é salvo, registrado ou arquivado. Esse evento tem o resultado `deleted`. Se a exclusão não for concluída, o evento nunca será enviado.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS para um evento `deleteVolume` bem-sucedido.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-012345678901",
    "detail-type": "EBS Volume Notification",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:012345678901:volume/vol-01234567"
    ],
    "detail": {
```

```
        "result": "deleted",
        "cause": "",
        "event": "deleteVolume",
        "request-id": "01234567-0123-0123-0123-0123456789ab"
    }
}
```

Anexar ou reanexar volumes (attachVolume, reattachVolume)

O evento `attachVolume` ou o `reattachVolume` será enviado à sua conta da AWS se ocorrer uma falha ao associar ou reassociar um volume a uma instância. Contudo, não é salvo, registrado ou arquivado. Se você usar uma Chave do KMS para criptografar um volume do EBS e a Chave do KMS se tornar inválida, o EBS emitirá um evento se a Chave do KMS for usada posteriormente para associar ou reassociar a uma instância, conforme mostrado nos exemplos abaixo.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `attachVolume` com falha. A causa da falha foi a exclusão pendente de uma Chave do KMS.

Note

A AWS pode tentar reanexar a um volume seguindo a manutenção rotineira do servidor.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "EBS Volume Notification",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
        "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
    ],
    "detail": {
        "event": "attachVolume",
        "result": "failed",
        "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab is pending deletion.",
        "request-id": ""
    }
}
```

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `reattachVolume` com falha. A causa da falha foi a exclusão pendente de uma Chave do KMS.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-0123456789ab",
    "detail-type": "EBS Volume Notification",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:0123456789ab:volume/vol-01234567",
        "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab"
    ],
    "detail": {

```

```
    "event": "reattachVolume",
    "result": "failed",
    "cause": "arn:aws:kms:us-east-1:0123456789ab:key/01234567-0123-0123-0123-0123456789ab
is pending deletion.",
    "request-id": ""
}
```

Eventos de snapshot do EBS

O Amazon EBS envia eventos ao CloudWatch Events quando ocorrem os eventos de volume a seguir.

Eventos

- [Criar snapshot \(createSnapshot\) \(p. 1483\)](#)
- [Criar snapshots \(createSnapshots\) \(p. 1483\)](#)
- [Copiar snapshot \(copySnapshot\) \(p. 1485\)](#)
- [Compartilhar snapshot \(shareSnapshot\) \(p. 1486\)](#)

Criar snapshot (createSnapshot)

O evento `createSnapshot` é enviado à sua conta da AWS quando uma ação para criar um snapshot termina. Contudo, não é salvo, registrado ou arquivado. Esse evento pode ter um resultado de `succeeded` ou `failed`.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS para um evento `createSnapshot` bem-sucedido. Na seção `detail`, o campo `source` contém o ARN do volume de origem. Os campos `startTime` e `endTime` indicam quando a criação do snapshot começou e foi concluída.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-012345678901",
    "detail-type": "EBS Snapshot Notification",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-west-2::snapshot/snap-01234567"
    ],
    "detail": {
        "event": "createSnapshot",
        "result": "succeeded",
        "cause": "",
        "request-id": "",
        "snapshot_id": "arn:aws:ec2:us-west-2::snapshot/snap-01234567",
        "source": "arn:aws:ec2:us-west-2::volume/vol-01234567",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "endTime": "yyyy-mm-ddThh:mm:ssZ"
    }
}
```

Criar snapshots (createSnapshots)

O evento `createSnapshots` é enviado à sua conta da AWS quando uma ação para criar um snapshot de vários volumes termina. Esse evento pode ter um resultado de `succeeded` ou `failed`.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido por EBS para um evento `createSnapshots` bem-sucedido. Na seção `detail`, o campo `source` contém os ARNs dos volumes de origem do conjunto de snapshots de vários volumes. Os campos `startTime` e `endTime` indicam quando a criação do snapshot começou e foi concluída.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Multi-Volume Snapshots Completion Status",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2::us-east-1:snapshot/snap-01234567",  
        "arn:aws:ec2::us-east-1:snapshot/snap-012345678"  
    ],  
    "detail": {  
        "event": "createSnapshots",  
        "result": "succeeded",  
        "cause": "",  
        "request-id": "",  
        "startTime": "yyyy-mm-ddThh:mm:ssZ",  
        "endTime": "yyyy-mm-ddThh:mm:ssZ",  
        "snapshots": [  
            {  
                "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",  
                "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",  
                "status": "completed"  
            },  
            {  
                "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",  
                "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",  
                "status": "completed"  
            }  
        ]  
    }  
}
```

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento `createSnapshots` com falha. A causa da falha foi a impossibilidade de conclusão de um ou mais snapshots do conjunto de snapshots de múltiplos volumes. Os valores de `snapshot_id` são os ARNs dos snapshots com falha. `startTime` e `endTime` representam quando a ação de criação de snapshots começou e terminou.

```
{  
    "version": "0",  
    "id": "01234567-0123-0123-0123-012345678901",  
    "detail-type": "EBS Multi-Volume Snapshots Completion Status",  
    "source": "aws.ec2",  
    "account": "012345678901",  
    "time": "yyyy-mm-ddThh:mm:ssZ",  
    "region": "us-east-1",  
    "resources": [  
        "arn:aws:ec2::us-east-1:snapshot/snap-01234567",  
        "arn:aws:ec2::us-east-1:snapshot/snap-012345678"  
    ],  
    "detail": {  
        "event": "createSnapshots",  
        "result": "failed",  
        "cause": "Snapshot snap-01234567 is in status error",  
        "request-id": "",  
        "startTime": "yyyy-mm-ddThh:mm:ssZ",  
        "endTime": "yyyy-mm-ddThh:mm:ssZ",  
        "snapshots": [  
            {  
                "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",  
                "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",  
                "status": "error"  
            },  
            {  
                "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",  
                "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",  
                "status": "error"  
            }  
        ]  
    }  
}
```

```
"endTime": "yyyy-mm-ddThh:mm:ssZ",
"snapshots": [
  {
    "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-01234567",
    "source": "arn:aws:ec2::us-east-1:volume/vol-01234567",
    "status": "error"
  },
  {
    "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678",
    "source": "arn:aws:ec2::us-east-1:volume/vol-012345678",
    "status": "error"
  }
]
```

Copiar snapshot (copySnapshot)

O evento copySnapshot é enviado à sua conta da AWS quando uma ação para copiar um snapshot termina. Contudo, não é salvo, registrado ou arquivado. Esse evento pode ter um resultado de succeeded ou failed.

Dados de eventos

A lista abaixo é um exemplo de um objeto JSON emitido pelo EBS após um evento copySnapshot bem-sucedido. O valor de snapshot_id é o ARN do snapshot recém-criado. Na seção detail, o valor de source é o ARN do snapshot de origem. startTime e endTime representam o início e o fim da ação copy-snapshot.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-01234567"
  ],
  "detail": {
    "event": "copySnapshot",
    "result": "succeeded",
    "cause": "",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2:us-west-2::snapshot/snap-01234567",
    "source": "arn:aws:ec2:eu-west-1::snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "Incremental": "True"
  }
}
```

A lista abaixo é um exemplo de um objeto JSON emitido por EBS depois de um evento copySnapshot com falha. A causa da falha era um ID de snapshot de origem inválido. O valor de snapshot_id é o nome de recurso da Amazon (ARN) do snapshot com falha. Na seção detail, o valor de source é o ARN do snapshot de origem. startTime e endTime representam o início e o fim da ação copy-snapshot.

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "EBS Snapshot Notification",
```

```
"source": "aws.ec2",
"account": "123456789012",
"time": "yyyy-mm-ddThh:mm:ssZ",
"region": "us-east-1",
"resources": [
    "arn:aws:ec2:us-west-2::snapshot/snap-01234567"
],
"detail": {
    "event": "copySnapshot",
    "result": "failed",
    "cause": "Source snapshot ID is not valid",
    "request-id": "",
    "snapshot_id": "arn:aws:ec2:us-west-2::snapshot/snap-01234567",
    "source": "arn:aws:ec2:eu-west-1::snapshot/snap-76543210",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ"
}
}
```

Compartilhar snapshot (shareSnapshot)

O evento shareSnapshot é enviado à sua conta da AWS quando outra conta compartilha um snapshot com ela. Contudo, não é salvo, registrado ou arquivado. O resultado é sempre succeeded.

Dados de eventos

Veja a seguir um exemplo de um objeto JSON emitido pelo EBS depois de um evento shareSnapshot concluído. Na seção detail, o valor de source é o número da conta da AWS do usuário que compartilhou o snapshot com você. startTime e endTime representam o início e o fim da ação shareSnapshot. O evento shareSnapshot é emitido somente quando um snapshot privado é compartilhado com outro usuário. Compartilhar um snapshot público não aciona o evento.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-012345678901",
    "detail-type": "EBS Snapshot Notification",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-west-2::snapshot/snap-01234567"
    ],
    "detail": {
        "event": "shareSnapshot",
        "result": "succeeded",
        "cause": "",
        "request-id": "",
        "snapshot_id": "arn:aws:ec2:us-west-2::snapshot/snap-01234567",
        "source": "012345678901",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "endTime": "yyyy-mm-ddThh:mm:ssZ"
    }
}
```

Eventos de modificação de volume do EBS

O Amazon EBS envia eventos modifyVolume para o CloudWatch Events quando um volume é modificado. Contudo, não é salvo, registrado ou arquivado.

```
{
```

```
"version": "0",
"id": "01234567-0123-0123-0123-012345678901",
"detail-type": "EBS Volume Notification",
"source": "aws.ec2",
"account": "012345678901",
"time": "yyyy-mm-ddThh:mm:ssZ",
"region": "us-east-1",
"resources": [
    "arn:aws:ec2:us-east-1:012345678901:volume/vol-03a55cf56513fa1b6"
],
"detail": {
    "result": "optimizing",
    "cause": "",
    "event": "modifyVolume",
    "request-id": "01234567-0123-0123-0123-0123456789ab"
}
}
```

Eventos de restauração rápida do snapshot do EBS

O Amazon EBS envia eventos para o CloudWatch Events quando o estado da restauração rápida do snapshot muda. Eventos são emitidos com base no melhor esforço.

A seguir estão dados de exemplo para esse evento.

```
{
    "version": "0",
    "id": "01234567-0123-0123-0123-012345678901",
    "detail-type": "EBS Fast Snapshot Restore State-change Notification",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1::snapshot/snap-03a55cf56513fa1b6"
    ],
    "detail": {
        "snapshot-id": "snap-1234567890abcdef0",
        "state": "optimizing",
        "zone": "us-east-1a",
        "message": "Client.UserInitiated - Lifecycle state transition"
    }
}
```

Os valores possíveis para state são enabling, optimizing, enabled, disabling e disabled.

Os valores possíveis para message são os seguintes:

`Client.InvalidSnapshot.InvalidState` - The requested snapshot transitioned to an invalid state (Error)

A solicitação para habilitar a restauração rápida do snapshot falhou e o estado mudou para disabling ou disabled. A restauração rápida do snapshot não pode ser habilitada para esse snapshot.

`Client.UserInitiated`

O estado fez a transição para enabling ou disabling.

`Client.UserInitiated` - Lifecycle state transition

O estado fez a transição para optimizing, enabled ou disabled.

`Server.InsufficientCapacity` - There was insufficient capacity available to satisfy the request

A solicitação para habilitar a restauração rápida do snapshot falhou por capacidade insuficiente, e o estado mudou para `disabling` ou `disabled`. Espere e tente novamente.

`Server.InternalError` - An internal error caused the operation to fail

A solicitação para habilitar a restauração rápida do snapshot falhou por erro interno, e o estado mudou para `disabling` ou `disabled`. Espere e tente novamente.

`Client.InvalidSnapshot.InvalidState` - The requested snapshot was deleted or access permissions were revoked

Foi feita a transição do estado de restauração rápida de snapshots para `disabling` ou `disabled` porque o snapshot foi excluído ou não compartilhado pelo proprietário do snapshot. A restauração rápida de snapshots não pode ser habilitada para um snapshot que tenha sido excluído ou não seja mais compartilhado com você.

Usar o AWS Lambda para lidar com o CloudWatch Events

Você pode usar o Amazon EBS e o CloudWatch Events para automatizar o fluxo de trabalho de backup de dados. Isso requer que você crie uma política do IAM, uma função do AWS Lambda para lidar com o evento e uma regra do Amazon CloudWatch Events que corresponde aos eventos de entrada e os roteia para a função do Lambda.

O procedimento a seguir usa o evento `createSnapshot` para copiar automaticamente um snapshot concluído em outra região para recuperação de desastres.

Como copiar um snapshot concluído em outra região

1. Crie uma política do IAM, como a mostrada no exemplo a seguir, para fornecer permissões para usar a ação `CopySnapshot` e gravá-la no log do CloudWatch Events. Atribua a política ao usuário do IAM que lidará com o evento do CloudWatch.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "logs>CreateLogGroup",  
                "logs>CreateLogStream",  
                "logs:PutLogEvents"  
            ],  
            "Resource": "arn:aws:logs:*:*:  
        },  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:CopySnapshot"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

2. Defina uma função no Lambda que estará disponível no console do CloudWatch. O exemplo de função do Lambda abaixo, escrito em Node.js, é invocado pelo CloudWatch quando um evento `createSnapshot` correspondente é emitido pelo Amazon EBS (significando que um snapshot foi concluído). Quando invocada, a função copia o snapshot de `us-east-2` em `us-east-1`.

```
// Sample Lambda function to copy an EBS snapshot to a different Region

var AWS = require('aws-sdk');
var ec2 = new AWS.EC2();

// define variables
var destinationRegion = 'us-east-1';
var sourceRegion = 'us-east-2';
console.log ('Loading function');

//main function
exports.handler = (event, context, callback) => {

    // Get the EBS snapshot ID from the CloudWatch event details
    var snapshotArn = event.detail.snapshot_id.split('/');
    const snapshotId = snapshotArn[1];
    const description = `Snapshot copy from ${snapshotId} in ${sourceRegion}.`;
    console.log ("snapshotId:", snapshotId);

    // Load EC2 class and update the configuration to use destination Region to
    // initiate the snapshot.
    AWS.config.update({region: destinationRegion});
    var ec2 = new AWS.EC2();

    // Prepare variables for ec2.modifySnapshotAttribute call
    const copySnapshotParams = {
        Description: description,
        DestinationRegion: destinationRegion,
        SourceRegion: sourceRegion,
        SourceSnapshotId: snapshotId
    };

    // Execute the copy snapshot and log any errors
    ec2.copySnapshot(copySnapshotParams, (err, data) => {
        if (err) {
            const errorMessage = `Error copying snapshot ${snapshotId} to Region
${destinationRegion}.`;
            console.log(errorMessage);
            console.log(err);
            callback(errorMessage);
        } else {
            const successMessage = `Successfully started copy of snapshot ${snapshotId}
to Region ${destinationRegion}.`;
            console.log(successMessage);
            console.log(data);
            callback(null, successMessage);
        }
    });
};

};
```

Para garantir que a sua função do Lambda esteja disponível no console do CloudWatch, crie-a na região onde o evento do CloudWatch ocorrerá. Para obter mais informações, consulte o [Guia do desenvolvedor do AWS Lambda](#).

3. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
4. Escolha Events (Eventos), Create rule (Criar regra), Select event source Selecionar origem do evento e Amazon EBS Snapshots.
5. Em Specific Event(s) (Eventos específicos), escolha createSnapshot e para Specific Result(s) (Resultados específicos), escolha succeeded (bem-sucedidos).
6. Em Rule target (Destino da regra), localize e escolha a função de exemplo que você criou anteriormente.

7. Escolha Target (Destino), Add Target (Adicionar destino).
8. Em Lambda function (Função do Lambda), selecione a função do Lambda que você criou anteriormente e escolha Configure details (Configurar detalhes).
9. Na página Configure rule details (Configurar detalhes da regra), digite valores para Name (Nome) e Description (Descrição). Marque a caixa de seleção Estado para ativar a função (definindo-a como Habilitado).
10. Selecione Criar regra.

A regra agora deve aparecer na guia Rules (Regras). No exemplo mostrado, o evento que você configurou deve ser emitido pelo EBS na próxima vez você copiar um snapshot.

Cotas do Amazon EBS

Para exibir as cotas de seus recursos do Amazon EBS, abra o console do Service Quotas em <https://console.aws.amazon.com/servicequotas/>. No painel de navegação, escolha AWS services (Produtos da AWS) e selecione Amazon Elastic Block Store(Amazon EBS).

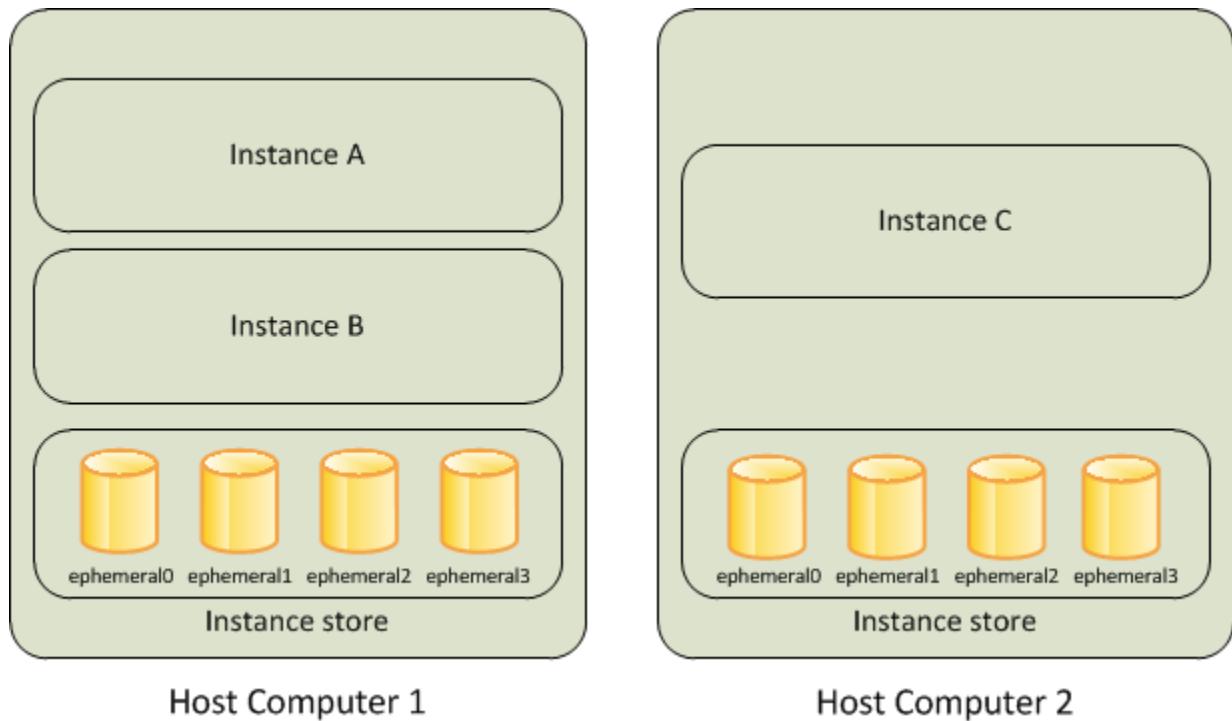
Para obter uma lista de cotas de serviço do Amazon EBS, consulte [Amazon Elastic Block Store endpoints and quotas](#) (Endpoints e cotas do Amazon Elastic Block Store) na AWS General Reference (Referência geral da AWS).

Armazenamento de instâncias do Amazon EC2

Um armazenamento de instâncias fornece armazenamento temporário em nível de bloco para a instância. Esse armazenamento está localizado em discos que estão anexados fisicamente ao computador host. O armazenamento de instâncias é ideal para o armazenamento temporário de informações que são alteradas frequentemente, como buffers, caches, dados de rascunho e outros conteúdos temporários ou para dados replicados em toda a frota de instâncias, como um grupo com平衡amento de carga de servidores Web.

Um armazenamento de instâncias consiste em um ou mais volumes de armazenamento de instâncias expostos como dispositivos de bloco. O tamanho de um armazenamento de instância e o número de dispositivos disponíveis varia por tipo de instância.

Os dispositivos virtuais para volumes de armazenamento de instâncias são `ephemeral[0-23]`. Tipos de instância que oferecem suporte a um volume de armazenamento de instâncias têm `ephemeral0`. Os tipos de instância que oferecem suporte a dois volumes de armazenamento de instâncias têm `ephemeral0` e `ephemeral1`, e assim por diante.



Tópicos

- [Vida útil do armazenamento de instâncias \(p. 1491\)](#)
- [Volumes de armazenamento de instâncias \(p. 1492\)](#)
- [Adicionar volumes de armazenamento de instâncias à instância do EC2 \(p. 1499\)](#)
- [Volumes de armazenamento de instâncias SSD \(p. 1503\)](#)

Vida útil do armazenamento de instâncias

Você pode especificar volumes de armazenamento de instâncias para uma instância somente quando a executa. Você não pode desanexar um volume de armazenamento de instâncias de uma instância e anexá-lo a outra instância.

Os dados em um armazenamento de instâncias persistem apenas durante a vida útil da instância associada. Se uma instância for reiniciada (intencionalmente ou accidentalmente), dados no armazenamento de instância persistirão. Contudo, os dados no armazenamento de instâncias serão perdidos em qualquer das seguintes circunstâncias:

- Falha em uma unidade de disco rígido subjacente
- A instância é parada
- A instância hiberna
- A instância é encerrada

Portanto, não dependa do armazenamento de instâncias para dados valiosos de longo prazo. Em vez disso, use um armazenamento físico de dados mais durável, como Amazon S3, Amazon EBS ou Amazon EFS.

Quando você para, hiberna ou encerra uma instância, cada bloco de armazenamento no armazenamento de instâncias é redefinido. Portanto, seus dados não podem ser acessados por meio do armazenamento de instâncias de outra instância.

Se você criar uma AMI de uma instância, os dados nos volumes de armazenamento de instâncias não serão preservados e não estarão presentes nos volumes de armazenamento de instâncias das instâncias executadas na AMI.

Se você alterar o tipo de instância, o armazenamento de instâncias não será vinculado ao novo tipo de instância. Para obter mais informações, consulte [Alterar o tipo de instância \(p. 244\)](#).

Volumes de armazenamento de instâncias

O tipo de instância determina o tamanho do armazenamento de instâncias disponível e o tipo de hardware usado para os volumes do armazenamento de instâncias. Os volumes do armazenamento de instâncias são incluídos como parte do custo por uso da instância. Você deve especificar os volumes do armazenamento de instâncias que você deseja usar ao executar a instância (exceto volumes de armazenamento de instâncias de NVMe, que estão disponíveis por padrão). Em seguida, formate e monte os volumes de armazenamento da instância antes de utilizá-los. Você não pode disponibilizar um volume de armazenamento de instâncias depois de executar a instância. Para obter mais informações, consulte [Adicionar volumes de armazenamento de instâncias à instância do EC2 \(p. 1499\)](#).

Alguns tipos de instância usam unidades de estado sólido (SSD) NVMe ou SATA para fornecer uma alta performance de E/S aleatória. Essa é uma boa opção quando você precisa de armazenamento com latência muito baixa, mas não precisa que os dados persistam quando a instância é encerrada, ou quando pode tirar proveito de arquiteturas tolerantes a falhas. Para obter mais informações, consulte [Volumes de armazenamento de instâncias SSD \(p. 1503\)](#).

Os dados nos volumes de armazenamento de instâncias do NVMe e alguns volumes de armazenamento de instâncias de HDD são criptografados em repouso. Para obter mais informações, consulte [Proteção de dados no Amazon EC2 \(p. 1134\)](#).

A tabela a seguir fornece a quantidade, o tamanho, o tipo e as otimizações de performance dos volumes de armazenamento de instâncias disponíveis em cada tipo de instância compatível. Para obter uma lista completa de tipos de instância, incluindo os tipos relacionados somente ao EBS, consulte [Tipos de instância do Amazon EC2](#).

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
c1.medium	1 x 350 GB	HDD	✓	
c1.xlarge	4 x 420 GB (1,6 TB)	HDD	✓	
c3.large	2 x 16 GB (32 GB)	SSD	✓	
c3.xlarge	2 x 40 GB (80 GB)	SSD	✓	
c3.2xlarge	2 x 80 GB (160 GB)	SSD	✓	
c3.4xlarge	2 x 160 GB (320 GB)	SSD	✓	
c3.8xlarge	2 x 320 GB (640 GB)	SSD	✓	
c5ad.large	1 x 75 GB	SSD de NVMe		✓
c5ad.xlarge	1 x 150 GB	SSD de NVMe		✓
c5ad.2xlarge	1 x 300 GB	SSD de NVMe		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
c5ad.4xlarge	2 x 300 GB (600 GB)	SSD de NVMe		✓
c5ad.8xlarge	2 x 600 GB (1,2 TB)	SSD de NVMe		✓
c5ad.12xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
c5ad.16xlarge	2 x 1.200 GB (2,4 TB)	SSD de NVMe		✓
c5ad.24xlarge	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
c5d.large	1 x 50 GB	SSD de NVMe		✓
c5d.xlarge	1 x 100 GB	SSD de NVMe		✓
c5d.2xlarge	1 x 200 GB	SSD de NVMe		✓
c5d.4xlarge	1 x 400 GB	SSD de NVMe		✓
c5d.9xlarge	1 x 900 GB	SSD de NVMe		✓
c5d.12xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
c5d.18xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
c5d.24xlarge	4 x 900 GB (3,6 TB)	SSD de NVMe		✓
c5d.metal	4 x 900 GB (3,6 TB)	SSD de NVMe		✓
cc2.8xlarge	4 x 840 GB (3.36 TB)	HDD	✓	
cr1.8xlarge	2 x 120 GB (240 GB)	SSD	✓	
d2.xlarge	3 x 2.000 GB (6 TB)	HDD		
d2.2xlarge	6 x 2.000 GB (12 TB)	HDD		
d2.4xlarge	12 x 2.000 GB (24 TB)	HDD		
d2.8xlarge	24 x 2.000 GB (48 TB)	HDD		
d3.xlarge	3 x 1.980 GB	HDD		
d3.2xlarge	6 x 1.980 GB	HDD		
d3.4xlarge	12 x 1.980 GB	HDD		
d3.8xlarge	24 x 1.980 GB	HDD		
d3en.large	1 x 13.980 GB	HDD		
d3en.xlarge	2 x 13.980 GB	HDD		
d3en.2xlarge	4 x 13.980 GB	HDD		
d3en.4xlarge	8 x 13.980 GB	HDD		
d3en.6xlarge	12 x 13.980 GB	HDD		
d3en.8xlarge	16 x 13.980 GB	HDD		

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
d3en.12xlarge	24 x 13.980 GB	HDD		
f1.2xlarge	1 x 470 GB	SSD de NVMe		✓
f1.4xlarge	1 x 940 GB	SSD de NVMe		✓
f1.16xlarge	4 x 940 GB (3.76 TB)	SSD de NVMe		✓
g2.2xlarge	1 x 60 GB	SSD	✓	
g2.8xlarge	2 x 120 GB (240 GB)	SSD	✓	
g4ad.xlarge	1 x 150 GB	SSD de NVMe		✓
g4ad.2xlarge	1 x 300 GB	SSD de NVMe		✓
g4ad.4xlarge	1 x 600 GB	SSD de NVMe		✓
g4ad.8xlarge	1 x 1.200 GB	SSD de NVMe		✓
g4ad.16xlarge	2 x 1.200 GB (2,4 TB)	SSD de NVMe		✓
g4dn.xlarge	1 x 125 GB	SSD de NVMe		✓
g4dn.2xlarge	1 x 225 GB	SSD de NVMe		✓
g4dn.4xlarge	1 x 225 GB	SSD de NVMe		✓
g4dn.8xlarge	1 x 900 GB	SSD de NVMe		✓
g4dn.12xlarge	1 x 900 GB	SSD de NVMe		✓
g4dn.16xlarge	1 x 900 GB	SSD de NVMe		✓
g4dn.metal	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
h1.2xlarge	1 x 2.000 GB (2 TB)	HDD		
h1.4xlarge	2 x 2.000 GB (4 TB)	HDD		
h1.8xlarge	4 x 2.000 GB (8 TB)	HDD		
h1.16xlarge	8 x 2.000 GB (16 TB)	HDD		
hs1.8xlarge	24 x 2.000 GB (48 TB)	HDD	✓	
i2.xlarge	1 x 800 GB	SSD		✓
i2.2xlarge	2 x 800 GB (1,6 TB)	SSD		✓
i2.4xlarge	4 x 800 GB (3.2 TB)	SSD		✓
i2.8xlarge	8 x 800 GB (6.4 TB)	SSD		✓
i3.large	1 x 475 GB	SSD de NVMe		✓
i3.xlarge	1 x 950 GB	SSD de NVMe		✓
i3.2xlarge	1 x 1.900 GB	SSD de NVMe		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
i3.4xlarge	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
i3.8xlarge	4 x 1.900 GB (7,6 TB)	SSD de NVMe		✓
i3.16xlarge	8 x 1.900 GB (15,2 TB)	SSD de NVMe		✓
i3.metal	8 x 1.900 GB (15,2 TB)	SSD de NVMe		✓
i3en.large	1 x 1.250 GB	SSD de NVMe		✓
i3en.xlarge	1 x 2.500 GB	SSD de NVMe		✓
i3en.2xlarge	2 x 2.500 GB (5 TB)	SSD de NVMe		✓
i3en.3xlarge	1 x 7.500 GB	SSD de NVMe		✓
i3en.6xlarge	2 x 7.500 GB (15 TB)	SSD de NVMe		✓
i3en.12xlarge	4 x 7.500 GB (30 TB)	SSD de NVMe		✓
i3en.24xlarge	8 x 7.500 GB (60 TB)	SSD de NVMe		✓
i3en.metal	8 x 7.500 GB (60 TB)	SSD de NVMe		✓
m1.small	1 x 160 GB	HDD	✓	
m1.medium	1 x 410 GB	HDD	✓	
m1.large	2 x 420 GB (840 GB)	HDD	✓	
m1.xlarge	4 x 420 GB (1,6 TB)	HDD	✓	
m2.xlarge	1 x 420 GB	HDD	✓	
m2.2xlarge	1 x 850 GB	HDD	✓	
m2.4xlarge	2 x 840 GB (1,68 TB)	HDD	✓	
m3.medium	1 x 4 GB	SSD	✓	
m3.large	1 x 32 GB	SSD	✓	
m3.xlarge	2 x 40 GB (80 GB)	SSD	✓	
m3.2xlarge	2 x 80 GB (160 GB)	SSD	✓	
m5ad.large	1 x 75 GB	SSD de NVMe		✓
m5ad.xlarge	1 x 150 GB	SSD de NVMe		✓
m5ad.2xlarge	1 x 300 GB	SSD de NVMe		✓
m5ad.4xlarge	2 x 300 GB (600 GB)	SSD de NVMe		✓
m5ad.8xlarge	2 x 600 GB (1,2 TB)	SSD de NVMe		✓
m5ad.12xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
m5ad.16xlarge	4 x 600 GB (2,4 TB)	SSD de NVMe		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
m5ad.24xlarge	4 x 900 GB (3.6 TB)	SSD de NVMe		✓
m5d.large	1 x 75 GB	SSD de NVMe		✓
m5d.xlarge	1 x 150 GB	SSD de NVMe		✓
m5d.2xlarge	1 x 300 GB	SSD de NVMe		✓
m5d.4xlarge	2 x 300 GB (600 GB)	SSD de NVMe		✓
m5d.8xlarge	2 x 600 GB (1,2 TB)	SSD de NVMe		✓
m5d.12xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
m5d.16xlarge	4 x 600 GB (2,4 TB)	SSD de NVMe		✓
m5d.24xlarge	4 x 900 GB (3.6 TB)	SSD de NVMe		✓
m5d.metal	4 x 900 GB (3.6 TB)	SSD de NVMe		✓
m5dn.large	1 x 75 GB	SSD de NVMe		✓
m5dn.xlarge	1 x 150 GB	SSD de NVMe		✓
m5dn.2xlarge	1 x 300 GB	SSD de NVMe		✓
m5dn.4xlarge	2 x 300 GB (600 GB)	SSD de NVMe		✓
m5dn.8xlarge	2 x 600 GB (1,2 TB)	SSD de NVMe		✓
m5dn.12xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
m5dn.16xlarge	4 x 600 GB (2,4 TB)	SSD de NVMe		✓
m5dn.24xlarge	4 x 900 GB (3.6 TB)	SSD de NVMe		✓
m5dn.metal	4 x 900 GB (3.6 TB)	SSD de NVMe		✓
p3dn.24xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
r3.large	1 x 32 GB	SSD		✓
r3.xlarge	1 x 80 GB	SSD		✓
r3.2xlarge	1 x 160 GB	SSD		✓
r3.4xlarge	1 x 320 GB	SSD		✓
r3.8xlarge	2 x 320 GB (640 GB)	SSD		✓
r5ad.large	1 x 75 GB	SSD de NVMe		✓
r5ad.xlarge	1 x 150 GB	SSD de NVMe		✓
r5ad.2xlarge	1 x 300 GB	SSD de NVMe		✓
r5ad.4xlarge	2 x 300 GB (600 GB)	SSD de NVMe		✓
r5ad.8xlarge	2 x 600 GB (1,2 TB)	SSD de NVMe		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
r5ad.12xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
r5ad.16xlarge	4 x 600 GB (2,4 TB)	SSD de NVMe		✓
r5ad.24xlarge	4 x 900 GB (3,6 TB)	SSD de NVMe		✓
r5d.large	1 x 75 GB	SSD de NVMe		✓
r5d.xlarge	1 x 150 GB	SSD de NVMe		✓
r5d.2xlarge	1 x 300 GB	SSD de NVMe		✓
r5d.4xlarge	2 x 300 GB (600 GB)	SSD de NVMe		✓
r5d.8xlarge	2 x 600 GB (1,2 TB)	SSD de NVMe		✓
r5d.12xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
r5d.16xlarge	4 x 600 GB (2,4 TB)	SSD de NVMe		✓
r5d.24xlarge	4 x 900 GB (3,6 TB)	SSD de NVMe		✓
r5d.metal	4 x 900 GB (3,6 TB)	SSD de NVMe		✓
r5dn.large	1 x 75 GB	SSD de NVMe		✓
r5dn.xlarge	1 x 150 GB	SSD de NVMe		✓
r5dn.2xlarge	1 x 300 GB	SSD de NVMe		✓
r5dn.4xlarge	2 x 300 GB (600 GB)	SSD de NVMe		✓
r5dn.8xlarge	2 x 600 GB (1,2 TB)	SSD de NVMe		✓
r5dn.12xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
r5dn.16xlarge	4 x 600 GB (2,4 TB)	SSD de NVMe		✓
r5dn.24xlarge	4 x 900 GB (3,6 TB)	SSD de NVMe		✓
r5dn.metal	4 x 900 GB (3,6 TB)	SSD de NVMe		✓
x1.16xlarge	1 x 1.920 GB	SSD		
x1.32xlarge	2 x 1.920 GB (3,84 TB)	SSD		
x1e.xlarge	1 x 120 GB	SSD		
x1e.2xlarge	1 x 240 GB	SSD		
x1e.4xlarge	1 x 480 GB	SSD		
x1e.8xlarge	1 x 960 GB	SSD		
x1e.16xlarge	1 x 1.920 GB	SSD		
x1e.32xlarge	2 x 1.920 GB (3,84 TB)	SSD		
z1d.large	1 x 75 GB	SSD de NVMe		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
<code>z1d.xlarge</code>	1 x 150 GB	SSD de NVMe		✓
<code>z1d.2xlarge</code>	1 x 300 GB	SSD de NVMe		✓
<code>z1d.3xlarge</code>	1 x 450 GB	SSD de NVMe		✓
<code>z1d.6xlarge</code>	1 x 900 GB	SSD de NVMe		✓
<code>z1d.12xlarge</code>	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
<code>z1d.metal</code>	2 x 900 GB (1,8 TB)	SSD de NVMe		✓

* Volumes anexados a determinadas instâncias sofrem uma penalidade de primeira gravação a menos que inicializados.

** Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 1504\)](#).

Para consultar informações de volume de armazenamento de instâncias usando a AWS CLI

Você pode usar o comando `describe-instance-types` da AWS CLI para exibir informações sobre um tipo de instância, como seus volumes de armazenamento de instâncias. O exemplo a seguir exibe o tamanho total do armazenamento de instâncias para todas as instâncias R5 com volumes de armazenamento de instâncias.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=r5*"
  "Name=instance-storage-supported,Values=true" --query "InstanceTypes[].[InstanceType,
  InstanceStorageInfo.TotalSizeInGB]" --output table
-----
|  DescribeInstanceTypes  |
+-----+-----+
| r5ad.24xlarge | 3600 |
| r5ad.12xlarge | 1800 |
| r5dn.8xlarge | 1200 |
| r5ad.8xlarge | 1200 |
| r5ad.large | 75 |
| r5d.4xlarge | 600 |
| . . .
| r5dn.2xlarge | 300 |
| r5d.12xlarge | 1800 |
+-----+-----+
```

O exemplo a seguir exibe os detalhes completos do armazenamento da instância para o tipo de instância especificado.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=r5d.4xlarge" --query
  "InstanceTypes[].[InstanceStorageInfo]"
```

O exemplo de resultado mostra que esse tipo de instância tem dois volumes SSD NVMe de 300 GB, para um total de 600 GB de armazenamento de instâncias.

```
[{
  "TotalSizeInGB": 600,
```

```
"Disks": [  
    {  
        "SizeInGB": 300,  
        "Count": 2,  
        "Type": "ssd"  
    }  
,  
    "NvmeSupport": "required"  
]
```

Adicionar volumes de armazenamento de instâncias à instância do EC2

Você especifica os volumes do EBS e os volumes de armazenamento de instâncias à instância usando um mapeamento de dispositivos de blocos. Cada entrada em um mapeamento de dispositivos de blocos inclui um nome de dispositivo e o volume para o qual ele é mapeado. O mapeamento de dispositivos de blocos padrão é especificado pela AMI que você usa. Como alternativa, você pode especificar um mapeamento de dispositivos de blocos para a instância ao executá-la.

Todos os volumes de armazenamento de instâncias de NVMe compatíveis com um tipo de instância são automaticamente enumerados e atribuídos a um nome de dispositivo durante a execução da instância. Incluí-los no mapeamento de dispositivos de blocos da AMI ou da instância não surtirá nenhum efeito. Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1513\)](#).

Um mapeamento de dispositivos de blocos sempre especifica o volume raiz da instância. O volume raiz é montado automaticamente. Para instâncias do Windows, o volume raiz deve ser um volume do Amazon EBS. O armazenamento de instâncias não é compatível com o volume raiz.

Você pode usar um mapeamento de dispositivos de blocos para especificar volumes do EBS adicionais ao executar a instância, ou pode anexar volumes do EBS adicionais depois que a instância está em execução. Para obter mais informações, consulte [Volumes do Amazon EBS \(p. 1245\)](#).

É possível especificar os volumes de armazenamento de instâncias para uma instância somente ao executá-la. Você não pode anexar volumes de armazenamento de instâncias depois de executar a instância.

Se você alterar o tipo de instância, o armazenamento de instâncias não será vinculado ao novo tipo de instância. Para obter mais informações, consulte [Alterar o tipo de instância \(p. 244\)](#).

O número e o tamanho de volumes de armazenamento de instâncias disponíveis variam por tipo de instância. Alguns tipos de instância não oferecem suporte a volumes de armazenamento de instâncias. Se o número de volumes de armazenamento de instâncias em um mapeamento de dispositivos de blocos exceder o número de volumes de armazenamento de instâncias disponível para uma instância, os volumes adicionais serão ignorados. Para obter mais informações sobre o suporte a volumes de armazenamento de instâncias com suporte de cada tipo de instância, consulte [Volumes de armazenamento de instâncias \(p. 1492\)](#).

Se o tipo de instância escolhido para a instância oferecer suporte aos volumes de armazenamento de instâncias não NVMe, adicione-os ao mapeamento de dispositivos de blocos da instância ao executá-la. Os volumes de armazenamento de instâncias NVMe estão disponíveis por padrão. Depois de executar uma instância, verifique se os volumes de armazenamento de instâncias da instância estão formatados e montados para poderem ser usados. O volume raiz de uma instância com suporte ao armazenamento de instâncias é montado automaticamente.

Tópicos

- [Adicionar volumes de armazenamento de instâncias a uma AMI \(p. 1500\)](#)

- [Adicionar volumes de armazenamento de instâncias a uma instância \(p. 1501\)](#)
- [Disponibilizar volumes de armazenamento de instâncias na instância \(p. 1502\)](#)

Adicionar volumes de armazenamento de instâncias a uma AMI

Você pode criar uma AMI com um mapeamento de dispositivos de blocos que inclua volumes de armazenamento de instâncias. Se você executar uma instância com um tipo de instância que ofereça suporte a volumes de armazenamento de instâncias e com uma AMI que especifique volumes de armazenamento de instâncias em seu mapeamento de dispositivos de blocos, a instância incluirá esses volumes de armazenamento de instâncias. Se o número de volumes de armazenamento de instâncias no mapeamento de dispositivos de blocos exceder o número de volumes de armazenamento de instâncias disponíveis para a instância, os volumes de armazenamento de instâncias adicionais serão ignorados.

Considerations

- Para instâncias M3, especifique volumes de armazenamento de instância no mapeamento de dispositivos de blocos da instância, não na AMI. O Amazon EC2 pode ignorar volumes de armazenamento de instância especificados apenas no mapeamento de dispositivos de blocos da AMI.
- Ao executar uma instância, você poderá omitir volumes de armazenamento de instâncias não NVMe especificados no mapeamento de dispositivos de blocos da AMI ou adicionar volumes de armazenamentos de instâncias.

New console

Para adicionar volumes de armazenamento de instâncias para uma AMI com suporte do Amazon EBS usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances e selecione a instância.
3. Escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).
4. Na página diálogo Create Image (Criar imagem), adicione um nome e uma descrição significativos para imagem.
5. Para cada volume de armazenamento de instâncias a ser adicionado, selecione Add volume (Adicionar volume), em Volume type (Tipo de volume) selecione um volume de armazenamento de instâncias, e em Device (Dispositivo), selecione um nome de dispositivo. (Para obter mais informações, consulte [Nomes de dispositivos em instâncias do Windows. \(p. 1512\)](#).) O número de volumes de armazenamento de instâncias disponíveis depende do tipo de instância. Para instâncias com volumes de armazenamento de instâncias de NVMe, o mapeamento de dispositivos desses volumes depende da ordem na qual o sistema operacional enumera os volumes.
6. Escolha Create Image (Criar imagem).

Old console

Para adicionar volumes de armazenamento de instâncias para uma AMI com suporte do Amazon EBS usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances e selecione a instância.
3. Escolha Ações, Imagem, Criar imagem.
4. Na caixa de diálogo Create Image, digite um nome e uma descrição significativos para a imagem.

5. Para cada volume de armazenamento da instância a ser adicionado, selecione Add New Volume, em Volume Type selecione um volume de armazenamento da instância, e em Device, selecione um nome de dispositivo. (Para obter mais informações, consulte [Nomes de dispositivos em instâncias do Windows. \(p. 1512\)](#).) O número de volumes de armazenamento de instâncias disponíveis depende do tipo de instância. Para instâncias com volumes de armazenamento de instâncias de NVMe, o mapeamento de dispositivos desses volumes depende da ordem na qual o sistema operacional enumera os volumes.
6. Escolha Create Image.

Para adicionar volumes de armazenamento de instâncias a uma AMI usando a linha de comando

Você pode usar um dos comandos a seguir. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- [create-image](#) ou [register-image](#) (AWS CLI)
- [New-EC2Image](#) e [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

Adicionar volumes de armazenamento de instâncias a uma instância

Quando você executa uma instância, o mapeamento de dispositivos de blocos padrão é fornecido pela AMI especificada. Se você precisar de volumes de armazenamento de instâncias adicionais, adicione-os à instância ao executá-la. Você também pode omitir dispositivos especificados no mapeamento de dispositivos de blocos da AMI.

Considerations

- Para instâncias do M3, você pode receber volumes de armazenamento de instâncias mesmo que você não os especifique no mapeamento de dispositivos de blocos da instância.
- Para instâncias do HS1, não importa quantos volumes de armazenamento de instâncias você especifica no mapeamento de dispositivos de blocos da AMI, o mapeamento de dispositivos de blocos de uma instância executada na AMI inclui automaticamente o número máximo de volumes de armazenamento de instâncias com suporte. Você deve remover explicitamente os volumes de armazenamento de instâncias que você não deseja no mapeamento de dispositivos de blocos da instância antes de executá-la.

Para atualizar o mapeamento de dispositivos de blocos de uma instância usando o console

1. Abra o console do Amazon EC2.
2. No painel, escolha Executar instância.
3. Na Step 1: Choose an Amazon Machine Image (AMI), selecione a AMI a ser usada e escolha Select.
4. Siga o assistente para concluir a Step 1: Choose an Amazon Machine Image (AMI), a Step 2: Choose an Instance Type e a Step 3: Configure Instance Details.
5. Na Step 4: Add Storage, modifique as entradas conforme necessário. Para cada volume de armazenamento da instância a ser adicionado, selecione Add New Volume, em Volume Type selecione um volume de armazenamento da instância, e em Device, selecione um nome de dispositivo. O número de volumes de armazenamento de instâncias disponíveis depende do tipo de instância.
6. Conclua o assistente e execute a instância.
7. (Opcional) Para visualizar os volumes de armazenamento de instâncias disponíveis na instância, abra o Gerenciamento de Disco do Windows.

Para atualizar o mapeamento de dispositivos de blocos de uma instância usando a linha de comando

Você pode usar um dos seguintes comandos de opções com o comando correspondente. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- `--block-device-mappings` com [run-instances](#) (AWS CLI)
- `-BlockDeviceMapping` com [New-EC2Instance](#) (AWS Tools for Windows PowerShell)

Disponibilizar volumes de armazenamento de instâncias na instância

Depois que você executa uma instância, os volumes de armazenamento de instâncias estão disponíveis para a instância, mas não será possível acessá-los até que você os monte. Para instâncias Linux, o tipo de instância determina quais volumes de armazenamento de instâncias são montados para você e quais estão disponíveis para que você mesmo monte. Em instâncias do Windows, o serviço EC2Config monta os volumes de armazenamento de instâncias para uma instância. O driver do dispositivo de blocos da instância atribui o nome real do volume ao montá-lo, e o nome atribuído pode ser diferente do nome recomendado pelo Amazon EC2.

Muitos volumes de armazenamento de instâncias são pré-formatados com o sistema de arquivos ext3. Os volumes de armazenamento de instâncias baseados em SSD que oferecem suporte à instrução TRIM não são pré-formatados com nenhum sistema de arquivos. No entanto, você pode formatar volumes com o sistema de arquivos de sua escolha depois de executar a instância. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 1504\)](#). Em instâncias do Windows, o serviço EC2Config reformata os volumes de armazenamento de instâncias com o sistema de arquivos NTFS.

Você pode confirmar se os dispositivos de armazenamento de instâncias estão disponíveis na própria instância usando metadados da instância. Para obter mais informações, consulte [Visualizar o mapeamento de dispositivos de blocos de instância para volumes de armazenamento de instâncias \(p. 1522\)](#).

Em instâncias do Windows, também é possível visualizar os volumes de armazenamento de instâncias usando o Gerenciamento de Disco do Windows. Para obter mais informações, consulte [Listar discos usando o Gerenciamento de disco \(p. 1528\)](#).

Como montar manualmente um volume de armazenamento de instâncias

1. Escolha Iniciar, insira Gerenciamento de computador e pressione Enter.
2. No painel esquerdo, escolha Gerenciamento de disco.
3. Se você for solicitado a inicializar o volume, escolha o volume a ser inicializado, selecione o tipo de partição necessário dependendo do seu caso de uso e escolha OK.
4. Na lista de volumes, clique com o botão direito do mouse no volume a ser montado e escolha Novo volume simples.
5. No assistente, escolha Avançar.
6. Na tela Especificar tamanho do volume, escolha Avançar para usar o tamanho máximo do volume. Como alternativa, escolha um tamanho de volume que esteja entre o espaço mínimo e o máximo em disco.
7. Na tela Atribuir uma letra ou um caminho de unidade, siga um destes procedimentos e escolha Avançar.
 - Para montar o volume com uma letra de unidade, escolha Atribuir a seguinte letra de unidade e escolha a letra da unidade a ser usada.
 - Para montar o volume como uma pasta, escolha Montar na seguinte pasta NTFS vazia e escolha Procurar para criar ou selecionar a pasta a ser usada.

- Para montar o volume sem uma letra ou um caminho de unidade, escolha Não atribuir uma letra ou um caminho de unidade.
8. Na tela Formatar partição, especifique se deseja ou não formatar o volume. Se você optar por formatar o volume, escolha o sistema de arquivos e o tamanho da unidade necessários e especifique um rótulo de volume.
 9. Escolha Avançar e Concluir.

Volumes de armazenamento de instâncias SSD

Como outros volumes de armazenamento de instâncias, você deve mapear os volumes de armazenamento de instância SSD para sua instância quando ela é executada. Os dados nos volumes de instância SSD persistem apenas durante a vida útil da instância do associada. Para obter mais informações, consulte [Adicionar volumes de armazenamento de instâncias à instância do EC2 \(p. 1499\)](#).

Volumes SSD de NVMe

Algumas instâncias oferecem volumes de armazenamento de instâncias de unidades de estado sólido (SSD) de memória expressa não volátil (NVMe). Para obter mais informações sobre o tipo de volume de armazenamento de instâncias compatível com cada tipo de instância, consulte [Volumes de armazenamento de instâncias \(p. 1492\)](#).

As AMIs do Windows da AWS mais recentes dos seguintes sistemas operacionais contêm os drivers do AWS NVMe usados para interagir com volumes de armazenamento de instâncias SSD que são expostos como dispositivos de bloco de NVMe para melhor performance:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Depois de se conectar à instância, você pode verificar se você vê os volumes de NVMe no Gerenciador de Disco. Na barra de ferramentas, abra o menu de contexto (clique com o botão direito do mouse) no logotipo do Windows e escolha Disk Management. No Windows Server 2008 R2, escolha Iniciar, Ferramentas administrativas, Gerenciamento do computador, Gerenciamento de disco.

As AMIs do Windows da AWS fornecidas pela Amazon incluem o driver do AWS NVMe. Se você não estiver usando as AMIs do Windows da AWS mais recentes, [instale o driver atual do AWS NVMe \(p. 580\)](#).

Os dados no armazenamento de instâncias de NVMe são criptografados usando uma criptografia de bloco XTS-AES-256 implementada em um módulo de hardware na instância. As chaves de criptografia são geradas usando o módulo de hardware e são exclusivas para cada dispositivo de armazenamento de instâncias de NVMe. Todas as chaves de criptografia são destruídas quando a instância é interrompida ou encerrada e não podem ser recuperadas. Você não pode desativar essa criptografia e não pode fornecer sua própria chave de criptografia.

Volumes SSD não NVMe

A instâncias a seguir oferecem suporte a volumes de armazenamento de instâncias que usam SSDs não NVMe para fornecer alta performance de E/S aleatória: C3, G2, I2, M3, R3 e X1. Para obter mais informações sobre o suporte a volumes de armazenamento de instâncias com suporte de cada tipo de instância, consulte [Volumes de armazenamento de instâncias \(p. 1492\)](#).

Suporte a TRIM do volume de armazenamento de instâncias

Alguns tipos de instâncias oferecem suporte a volumes SSD com TRIM. Para obter mais informações, consulte [Volumes de armazenamento de instâncias \(p. 1492\)](#).

As instâncias que executam o Windows Server 2012 R2 são compatíveis com TRIM a partir do driver AWS PV versão 7.3.0. As instâncias que executam versões anteriores do Windows Server não são compatíveis com TRIM.

Os volumes de armazenamento de instâncias que oferecem suporte ao TRIM são aparados completamente antes de serem alocados à instância. Esses volumes não estão formatados com um sistema de arquivos quando uma instância é iniciada, portanto, você deve formatá-los para que possam ser montados e usados. Para obter acesso mais rápido a esses volumes, você deve ignorar a operação TRIM ao formatá-los. No Windows, para desativar temporariamente o suporte TRIM durante a formatação inicial, use o comando `fsutil behavior set DisableDeleteNotify 1`. Após a conclusão da formatação, reactive o suporte TRIM usando `fsutil behavior set DisableDeleteNotify 0`.

Com volumes de armazenamento de instâncias que oferecem suporte ao TRIM, você pode usar o comando TRIM para notificar o controlador de SSD quando você não precisa mais dos dados que gravou. Isso fornece ao controlador mais espaço livre, o que pode reduzir a amplificação da gravação e aumentar a performance. No Windows, use o comando `fsutil behavior set DisableDeleteNotify 0` para garantir que o suporte TRIM esteja habilitado durante a operação normal.

Armazenamento de arquivos

O armazenamento de arquivos na nuvem é um método de armazenamento de dados na nuvem que permite que servidores e aplicações accessem os dados por meio de sistemas de arquivos compartilhados. Essa compatibilidade faz do armazenamento de arquivos na nuvem uma opção ideal para workloads que dependem de sistemas de arquivos compartilhados e oferece simplicidade de integração, sem alterações de código.

Há muitas soluções de armazenamento de arquivos, desde um servidor de arquivos de nó único em uma instância de computação que usa armazenamento em blocos como base sem escalabilidade ou poucas redundâncias para proteger os dados a uma solução clusterizada do tipo "faça você mesmo" ou a uma solução totalmente gerenciada. O conteúdo a seguir apresenta alguns dos serviços de armazenamento fornecidos pela AWS para uso com o Windows.

Tópicos

- [Usar o Amazon S3 com a Amazon EC2 \(p. 1504\)](#)
- [Usar o Amazon EFS com o Amazon EC2 \(p. 1506\)](#)
- [Usar o FSx for Windows File Server com a Amazon EC2 \(p. 1506\)](#)

Usar o Amazon S3 com a Amazon EC2

O Amazon S3 é um repositório de dados da Internet. O Amazon S3 fornece acesso a uma infraestrutura de armazenamento de dados confiável, rápida e econômica. Ele foi projetado para facilitar a computação em escala da Web habilitando o armazenamento e a recuperação de qualquer quantidade de dados, a qualquer momento, no Amazon EC2 ou em qualquer lugar na Web. O Amazon S3 armazena objetos de dados de forma redundante em vários dispositivos em várias instalações e permite acesso simultâneo de leitura ou gravação a esses objetos de dados por muitos clientes distintos ou threads de aplicações. Você pode usar os dados redundantes armazenados no Amazon S3 para recuperação rápida e confiável em caso de falhas da instância ou da aplicação.

O Amazon EC2 usa o Amazon S3 para armazenar imagens de máquina da Amazon (AMIs). Você usa AMIs para executar instâncias do EC2. Em caso de falha da instância, você pode usar a AMI armazenada

para executar outra instância imediatamente, permitindo dessa forma uma recuperação rápida e a continuidade dos negócios.

O Amazon EC2 também usa o Amazon S3 para armazenar snapshots (cópias de backup) dos volumes de dados. Você pode usar snapshots para recuperar dados de forma rápida e confiável em caso de falhas da aplicação ou do sistema. Você também pode usar Snapshots como uma linha de base para criar vários novos volumes de dados, expandir o tamanho de um volume de dados existente ou mover volumes de dados entre várias zonas de disponibilidade, tornando seu uso de dados altamente escalável. Para obter mais informações sobre como usar volumes de dados e snapshots, consulte [Amazon Elastic Block Store \(p. 1243\)](#).

Os objetos são as entidades fundamentais armazenadas no Amazon S3. Cada objeto armazenado no Amazon S3 é contido em um bucket. Os buckets organizam o namespace do Amazon S3 no nível mais alto e identificam a conta responsável por esse armazenamento. Os buckets do Amazon S3 são semelhantes aos nomes de domínio da Internet. Os objetos armazenados em buckets têm um valor de chave exclusiva e são recuperados usando um URL. Por exemplo, se um objeto com um valor de chave `/photos/mygarden.jpg` estiver armazenado no bucket `DOC-EXAMPLE-BUCKET1`, ele será endereçável usando a URL `https://DOC-EXAMPLE-BUCKET1.s3.amazonaws.com/photos/mygarden.jpg`.

Para obter mais informações sobre os recursos do Amazon S3, consulte a [página do produto Amazon S3](#).

Exemplos de uso

Considerando os benefícios do Amazon S3 para armazenamento, você poderia usar esse serviço para armazenar arquivos e conjuntos de dados para uso com instâncias do EC2. Há várias maneiras de mover dados do Amazon S3 para suas instâncias e vice-versa. Além dos exemplos discutidos a seguir, há várias ferramentas escritas por pessoas que você pode usar para acessar seus dados no Amazon S3, no computador ou na instância. Algumas das comuns são discutidas nos fóruns de discussão da AWS.

Se você tiver permissão, poderá copiar um arquivo entre o Amazon S3 e sua instância usando um dos seguintes métodos.

AWS Tools for Windows PowerShell

As instâncias Windows têm o benefício de um navegador gráfico que pode ser usado para acessar o console do Amazon S3 diretamente. No entanto, para fins de script, os usuários do Windows também podem usar o [AWS Tools for Windows PowerShell](#) para mover objetos para/do Amazon S3.

Use o seguinte comando para copiar um objeto do Amazon S3 em sua instância do Windows.

```
PS C:\> Copy-S3Object -BucketName my_bucket -Key path-to-file -LocalFile my_copied_file.ext
```

AWS Command Line Interface

A AWS Command Line Interface (AWS CLI) é uma ferramenta unificada para gerenciar os serviços da AWS. A AWS CLI permite que os usuários se autentiquem e façam download de itens restritos no Amazon S3 e também façam upload de itens. Para obter mais informações sobre, por exemplo, como instalar e configurar as ferramentas, consulte a [página de detalhes do AWS Command Line Interface](#).

O comando aws s3 cp é semelhante ao comando Unix cp. Você pode copiar arquivos do Amazon S3 para sua instância, copiar arquivos de sua instância para o Amazon S3, e copiar arquivos de um local do Amazon S3 para outro.

Use o comando a seguir para copiar um objeto do Amazon S3 em sua instância.

```
aws s3 cp s3://my_bucket/my_folder/my_file.ext my_copied_file.ext
```

Use o comando a seguir para copiar um objeto de sua instância de volta para o Amazon S3.

```
aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

O comando aws s3 sync pode sincronizar um bucket inteiro do Amazon S3 com um diretório local. Isso pode ser útil para fazer download de um banco de dados e manter a cópia local atualizada com o banco remoto. Se tiver as permissões adequadas no bucket do Amazon S3, você poderá enviar o backup do diretório local por push para a nuvem quando concluir invertendo os locais de origem e de destino no comando.

Use o seguinte comando para fazer download de todo o bucket do Amazon S3 para um diretório local em sua instância.

```
aws s3 sync s3://remote_S3_bucket local_directory
```

API do Amazon S3

Se você for um desenvolvedor, poderá usar uma API para acessar dados no Amazon S3. Para obter mais informações, consulte o [Amazon Simple Storage Service Developer Guide](#) (Guia do desenvolvedor do Amazon Simple Storage Service). Você pode usar essa API e os respectivos exemplos para ajudar a desenvolver sua aplicação e a integrá-la com outras APIs e SDKs, como a interface boto do Python.

Usar o Amazon EFS com o Amazon EC2

O Amazon EFS fornece armazenamento de arquivos escalável para uso com o Amazon EC2. Você pode usar um sistema de arquivos de EFS como uma fonte de dados comum para cargas de trabalho e aplicativos em execução em várias instâncias. Para obter mais informações, consulte a [página do produto Amazon Elastic File System](#).

Important

O Amazon EFS não tem suporte em instâncias Windows.

Para usar o Amazon EFS com uma instância do Linux, consulte [Amazon Elastic File System \(Amazon EFS\)](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Usar o FSx for Windows File Server com a Amazon EC2

O FSx for Windows File Server fornece servidores de arquivos do Windows totalmente gerenciados, apoiados por um sistema totalmente nativo de arquivos do Windows, com os recursos, a performance e a compatibilidade para operar lift-and-shift com facilidade em aplicações empresariais para a AWS.

O Amazon FSx oferece suporte a um amplo conjunto de workloads corporativas do Windows com armazenamento de arquivos totalmente gerenciado criado no Microsoft Windows Server. O Amazon FSx tem suporte nativo para recursos do sistema de arquivos Windows e para o protocolo SMB (Server Message Block) padrão do setor para acessar o armazenamento de arquivos em uma rede. O Amazon FSx é otimizado para aplicações corporativas na Nuvem AWS, com compatibilidade nativa do Windows, performance e recursos corporativos e latências consistentes abaixo de um milissegundo.

Com o armazenamento de arquivos no Amazon FSx, o código, as aplicações e as ferramentas que os desenvolvedores e administradores do Windows usam hoje em dia podem continuar a funcionar sem alterações. As workloads e aplicações do Windows que são ideais para o Amazon FSx incluem workloads de aplicações empresariais, diretórios iniciais, serviço Web, gerenciamento de conteúdo, análise de dados, configurações de criação de software e processamento de mídia.

Como um serviço totalmente gerenciado, o FSx for Windows File Server elimina os custos administrativos indiretos de configurar e provisionar servidores de arquivos e volumes de armazenamento. Além disso, ele

mantém o software do Windows atualizado, detecta e resolve falhas de hardware e realiza backups. Ele também fornece integração avançada com outros produtos da AWS, incluindo o AWS Directory Service para Microsoft Active Directory, Amazon WorkSpaces, AWS Key Management Service e AWS CloudTrail.

Para obter mais informações, consulte o [Manual do usuário do FSx for Windows File Server](#). Para obter informações sobre preços, consulte [Preços do FSx for Windows File Server](#).

Limites de volumes de instância

O número máximo de volumes que sua instância pode ter depende do sistema operacional e do tipo de instância. Ao considerar quantos volumes adicionar à sua instância, você deve considerar se precisa de largura de banda de E/S aprimorada ou maior capacidade de armazenamento.

Tópicos

- [Limites de volumes do Sistema Nitro \(p. 1507\)](#)
- [Limites de volumes específicos do Windows \(p. 1507\)](#)
- [Largura de banda x capacidade \(p. 1508\)](#)

Limites de volumes do Sistema Nitro

As instâncias criadas no [Sistema Nitro \(p. 154\)](#) oferecem suporte a um número máximo de anexos, que são compartilhados entre interfaces de rede, volumes do EBS e volumes de armazenamento de instâncias NVMe. Cada instância tem pelo menos um anexo de interface de rede. Os volumes de armazenamento de instâncias de NVMe são anexados automaticamente. Para obter mais informações, consulte [Interfaces de rede elástica \(p. 1002\)](#) e [Volumes de armazenamento de instâncias \(p. 1492\)](#).

A maioria dessas instâncias oferece suporte a um máximo de 28 anexos. Por exemplo, se você não tiver anexos de interface de rede adicionais em uma instância somente do EBS, poderá anexar até 27 volumes do EBS a ela. Se tiver uma interface de rede adicional em uma instância com dois volumes de armazenamento de instâncias de NVMe, você poderá anexar 24 volumes do EBS a ela.

Para outras instâncias, os seguintes limites se aplicam:

- As instâncias d3.8xlarge e d3en.12xlarge oferecem suporte a um máximo de 3 volumes do EBS.
- A maioria das instâncias bare metal oferece suporte a um máximo de 31 volumes do EBS.
- As instâncias virtualizadas de alta memória oferecem suporte a um máximo de 27 volumes do EBS.
- As instâncias bare metal de alta memória oferecem suporte a um máximo de 19 volumes do EBS.

Se você iniciou uma instância bare metal de alta memória u-6tb1.metal, u-9tb1.metal ou u-12tb1.metal antes de 12 de março de 2020, ela oferece suporte a um máximo de 14 volumes do EBS. Para anexar até 19 volumes do EBS a uma dessas instâncias, entre em contato com a equipe de sua conta para atualizar a instância sem custo adicional.

Limites de volumes específicos do Windows

A tabela a seguir mostra os limites de volumes para instâncias Windows com base no driver usado. Observe que esses números incluem o volume raiz, mas os volumes do EBS e os volumes de armazenamento de instâncias anexados.

Important

Anexar mais do que os volumes a seguir a uma instância Windows tem suporte somente em uma base de melhor esforço e não é garantido.

Driver	Solicitação de volume
AWS PV	26
Citrix PV	26
Red Hat PV	17

Não recomendamos a anexação de mais de 26 volumes a uma instância Windows com drivers AWS PV ou Citrix PV, pois é provável que isso cause problemas de performance.

Para determinar quais drivers PV sua instância está usando ou atualizar sua instância Windows do Red Hat para drivers Citrix PV, consulte [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#).

Para obter mais informações sobre como nomes de dispositivos se relacionaram a volumes, consulte [Mapear discos para volumes na sua instância Windows \(p. 1524\)](#).

Largura de banda x capacidade

Para casos de uso de largura de banda consistentes e previsíveis, use as instâncias de conectividade de rede de 10 gigabits ou otimizadas para EBS e volumes do Finalidade geral (SSD) ou do Provisioned IOPS SSD. Siga as orientações em [Instâncias otimizadas para Amazon EBS \(p. 1440\)](#) para fazer a correspondência entre a IOPS provisionada para seus volumes e a largura de banda disponível para suas instâncias a fim de obter a performance máxima. Para configurações de RAID, muitos administradores acham que matrizes com mais de 8 volumes prejudicam a performance devido à maior sobrecarga de E/S. Teste a performance de aplicações individuais e ajuste, se necessário.

Volume do dispositivo raiz da instância do Amazon EC2

Quando você executa uma instância, o volume do dispositivo raiz contém a imagem usada para iniciar a instância. Quando você executa uma instância do Windows, um volume do dispositivo raiz do EBS é criado de um snapshot do EBS e anexado à instância.

Tópicos

- [Configurar o volume raiz para persistir \(p. 1508\)](#)
- [Confirmar que um volume raiz está configurado para persistir \(p. 1510\)](#)
- [Alterar o tamanho inicial do volume raiz \(p. 1511\)](#)

Configurar o volume raiz para persistir

Por padrão, o volume raiz é excluído quando a instância é encerrada (o `DeleteOnTermination` atributo é `true`). Usando o console, você pode alterar `DeleteOnTermination` quando executar uma instância. Para alterar esse atributo para uma instância existente, use a linha de comando.

Tópicos

- [Configurar o volume raiz para persistir durante a execução da instância \(p. 1509\)](#)
- [Configurar o volume raiz para persistir em uma instância existente \(p. 1510\)](#)

Configurar o volume raiz para persistir durante a execução da instância

Você pode configurar o volume raiz para persistir ao executar uma instância usando o console do Amazon EC2 ou as ferramentas de linha de comando.

Console

Como configurar o volume raiz para persistir ao executar uma instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias) e Launch instances (Executar instâncias).
3. Na página Choose an Amazon Machine Image (AMI) (Escolha uma imagem de máquina da Amazon), selecione as AMIs a serem usadas e escolha Select (Selecionar).
4. Siga o assistente para preencher as páginas Choose an Instance Type e Configure Instance Details.
5. Na página Add Storage (Adicionar armazenamento), desmarque Delete On Termination (Excluir ao encerrar) no volume raiz.
6. Preencha as páginas restantes do assistente e escolha Launch (Executar).

AWS CLI

Como configurar o volume raiz para persistir ao executar uma instância usando o AWS CLI

Use o comando `run-instances` e inclua um mapeamento de dispositivo de bloco que define o atributo `DeleteOnTermination` como `false`.

```
C:\> aws ec2 run-instances --block-device-mappings file://mapping.json ...other parameters...
```

Especifique o seguinte em `mapping.json`.

```
[  
  {  
    "DeviceName": "/dev/sda1",  
    "Ebs": {  
      "DeleteOnTermination": false  
    }  
  }  
]
```

Tools for Windows PowerShell

Como configurar o volume raiz para persistir ao executar uma instância usando o Tools for Windows PowerShell

Use o comando `New-EC2Instance` e inclua um mapeamento de dispositivo de bloco que define o atributo `DeleteOnTermination` como `false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsBlockDevice  
C:\> $ebs.DeleteOnTermination = $false  
C:\> $bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping  
C:\> $bdm.DeviceName = "dev/xvda"  
C:\> $bdm.Ebs = $ebs  
C:\> New-EC2Instance -ImageId ami-0abcdef1234567890 -BlockDeviceMapping $bdm ...other parameters...
```

Configurar o volume raiz para persistir em uma instância existente

Você pode configurar o volume raiz para persistir em uma instância em execução usando apenas as ferramentas de linha de comando.

AWS CLI

Como configurar o volume raiz para persistir em uma instância existente usando o AWS CLI

Use o comando [modify-instance-attribute](#) com um mapeamento de dispositivo de blocos que define o atributo `DeleteOnTermination` como `false`.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file:/mapping.json
```

Especifique o seguinte em `mapping.json`.

```
[  
  {  
    "DeviceName": "/dev/xvda",  
    "Ebs": {  
      "DeleteOnTermination": false  
    }  
  }  
]
```

Tools for Windows PowerShell

Como configurar o volume raiz para persistir em uma instância existente usando o AWS Tools for Windows PowerShell

Use o comando [Edit-EC2InstanceAttribute](#) com um mapeamento de dispositivo de blocos que define o atributo `DeleteOnTermination` como `false`.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification  
C:\> $ebs.DeleteOnTermination = $false  
C:\> $bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification  
C:\> $bdm.DeviceName = /dev/xvda  
C:\> $bdm.Ebs = $ebs  
C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -BlockDeviceMapping $bdm
```

Confirmar que um volume raiz está configurado para persistir

Você pode confirmar que um volume raiz está configurado para persistir usando o console do Amazon EC2 ou as ferramentas da linha de comando.

New console

Como confirmar se um volume raiz está configurado para persistir usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância.
3. Na guia Storage (Armazenamento), em Block devices (Dispositivos de blocos), localize a entrada do volume raiz. Se a opção Delete on termination (Excluir ao encerrar) for No, o volume será configurado para persistir.

Old console

Como confirmar se um volume raiz está configurado para persistir usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância.
3. Na guia Description (Descrição), escolha a entrada para o Root device (Dispositivo raiz). Se a opção Delete on termination (Excluir ao encerrar) for False, o volume será configurado para persistir.

AWS CLI

Como confirmar que um volume raiz está configurado para persistir usando a AWS CLI

Use o comando `describe-instances` e verifique se o atributo `DeleteOnTermination` no elemento de resposta `BlockDeviceMappings` está definido como `false`.

```
C:\> aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

```
...
"BlockDeviceMappings": [
{
    "DeviceName": "/dev/sda1",
    "Ebs": {
        "Status": "attached",
        "DeleteOnTermination": false,
        "VolumeId": "vol-1234567890abcdef0",
        "AttachTime": "2013-07-19T02:42:39.000Z"
    }
}
...]
```

Tools for Windows PowerShell

Como confirmar que um volume raiz está configurado para persistir usando a AWS Tools for Windows PowerShell

Use o `Get-EC2Instance` e verifique se o atributo `DeleteOnTermination` no elemento de resposta `BlockDeviceMappings` está definido como `false`.

```
C:\> (Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Alterar o tamanho inicial do volume raiz

Por padrão, o tamanho do volume raiz é determinado pelo tamanho do snapshot. É possível aumentar o tamanho inicial do volume raiz usando o mapeamento de dispositivos de blocos da instância da seguinte forma.

1. Determine o nome do dispositivo do volume raiz especificado na AMI, conforme descrito em [Visualizar os volumes do EBS em um mapeamento de dispositivo de blocos da AMI \(p. 1519\)](#).
2. Confirme o tamanho do snapshot especificado no mapeamento de dispositivos de blocos da AMI, conforme descrito em [Exibir informações do snapshot do Amazon EBS \(p. 1322\)](#).
3. Substitua o tamanho do volume raiz usando o mapeamento de dispositivos de blocos da instância, conforme descrito em [Atualizar o mapeamento de dispositivos de blocos ao executar uma instância \(p. 1520\)](#), especificando um tamanho de volume maior que o tamanho do snapshot.

Por exemplo, a entrada a seguir para o mapeamento de dispositivos de blocos da instância aumenta o tamanho do volume raiz /dev/xvda para 100 GiB. É possível omitir o ID do snapshot no mapeamento de dispositivos de blocos da instância porque o ID do snapshot já está especificado no mapeamento dos dispositivos de blocos da AMI.

```
{  
    "DeviceName": "/dev/xvda",  
    "Ebs": {  
        "VolumeSize": 100  
    }  
}
```

Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1513\)](#).

Nomes de dispositivos em instâncias do Windows.

Quando você anexa um volume à instância, você inclui um nome de dispositivo para o volume. Esse nome de dispositivo é usado pelo Amazon EC2. O driver do dispositivo de blocos da instância atribui o nome real do volume ao montá-lo, e o nome atribuído pode ser diferente do nome usado pelo Amazon EC2.

O número de volumes que a instância pode suportar é determinado pelo sistema operacional. Para obter mais informações, consulte [Limites de volumes de instância \(p. 1507\)](#).

Tópicos

- [Nomes de dispositivos disponíveis \(p. 1512\)](#)
- [Considerações sobre nomes de dispositivos \(p. 1513\)](#)

Para obter informações sobre nomes de dispositivos em instâncias do Linux, consulte [Nomenclatura de dispositivos em instâncias do Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Nomes de dispositivos disponíveis

As AMIs do Windows usam um dos seguintes conjuntos de drivers para permitir acesso ao hardware virtualizado: AWS PV, Citrix PV e RedHat PV. Para obter mais informações, consulte [Drivers paravirtuais para as instâncias do Windows \(p. 559\)](#).

A tabela a seguir lista os nomes de dispositivo disponíveis que podem ser especificados em um mapeamento de dispositivo de bloco ou ao associar um volume do EBS.

Tipo de driver	Disponível	Reservado para raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
AWS PV, Citrix PV	xvd[b-z]	/dev/sda1	xvd[f-z] *	xvdc[a-x]

Tipo de driver	Disponível	Reservado para raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
	xdv[b-c][a-z] <code>/dev/sda1</code> <code>/dev/sd[b-e]</code>			<code>xdv[a-e]</code> **
Red Hat PV	<code>xdv[a-z]</code> <code>xdv[b-c][a-z]</code> <code>/dev/sda1</code> <code>/dev/sd[b-e]</code>	<code>/dev/sda1</code>	<code>xdv[f-p]</code>	<code>xvdc[a-x]</code> <code>xvd[a-e]</code>

* Para Citrix PV e Red Hat PV, se você mapear um volume do EBS com o nome `xvda`, o Windows não reconhece o volume (o volume é visível para AWS PV ou AWS NVMe).

** Os volumes de armazenamento de instâncias NVMe são automaticamente enumerados e atribuídos a um letra de unidade do Windows.

Para obter mais informações sobre volumes de armazenamento de instâncias, consulte [Armazenamento de instâncias do Amazon EC2 \(p. 1490\)](#). Para obter mais informações sobre volumes do EBS do NVMe (instâncias baseadas em Nitro), incluindo como identificar o dispositivo do EBS, consulte [Amazon EBS e NVMe em instâncias Windows \(p. 1438\)](#).

Considerações sobre nomes de dispositivos

Lembre-se do seguinte ao selecionar um nome de dispositivo:

- Embora você possa anexar os volumes do EBS usando nomes de dispositivos usados para volumes de armazenamento da instância, recomendamos enfaticamente que você não o faça porque o comportamento poderá ser imprevisível.
- O número de volumes de armazenamento de instâncias NVMe de uma instância depende do tamanho da instância. Os volumes de armazenamento de instâncias NVMe são automaticamente enumerados e recebem uma letra de unidade do Windows.
- As AMIs do Windows da AWS vêm com software adicional que prepara uma instância quando na primeira inicialização. Ele é o serviço EC2Config (AMIs do Windows de versões anteriores ao Windows Server 2016) ou EC2Launch (Windows Server 2016 e posterior). Após o mapeamento nas unidades, os dispositivos são inicializados e montados. A unidade raiz é inicializada e montada como C: \. Por padrão, quando um volume do EBS é anexado a uma instância do Windows, ele poderá ser mostrado como qualquer letra de unidade na instância. É possível alterar as configurações para definir as letras dos volumes de acordo com suas especificações. Para volumes de armazenamento de instâncias, o padrão depende do driver. AWS Os drivers PV e Citrix PV atribuem aos volumes de armazenamento de instância letras que vão de Z: a A: Os drivers do Red Hat atribuem aos volumes de armazenamento da instância letras de unidades que vão de D: a Z:. Para obter mais informações, consulte [Configurar uma instância do Windows usando o serviço EC2Config \(p. 530\)](#), [Configurar uma instância do Windows usando o EC2Launch \(p. 522\)](#) e [Mapear discos para volumes na sua instância Windows \(p. 1524\)](#).

Mapeamentos de dispositivos de blocos

Cada instância que você executa tem um volume de dispositivo raiz associado, seja um volume do Amazon EBS ou um volume de armazenamento de instâncias. Use o mapeamento de dispositivos de

blocos para especificar mais volumes do EBS ou volumes de armazenamento de instâncias para anexar a uma instância quando ela for executada. Você pode ligar volumes adicionais do EBS a uma instância em execução; consulte [Vincular um volume de Amazon EBS a uma instância \(p. 1271\)](#). Contudo, a única forma de associar volumes de armazenamento de instâncias a uma instância é usar o mapeamento de dispositivos de blocos para anexá-los à medida que a instância é executada.

Para obter mais informações sobre volumes de dispositivos raiz, consulte [Volume do dispositivo raiz da instância do Amazon EC2 \(p. 1508\)](#).

Tópicos

- [Conceitos de mapeamento de dispositivos de blocos \(p. 1514\)](#)
- [Mapeamento de dispositivos de blocos da AMI \(p. 1517\)](#)
- [Mapeamento de dispositivos de blocos de instância \(p. 1519\)](#)

Conceitos de mapeamento de dispositivos de blocos

Um dispositivo de blocos é um dispositivo de armazenamento que move dados em sequências de bytes ou de bits (blocos). Esses dispositivos oferecem suporte ao acesso aleatório e geralmente usam E/S em buffer. Os exemplos incluem discos rígidos, unidades de CD-ROM e pen-drives. Um dispositivo de blocos pode ser fisicamente ligado a um computador ou acessado remotamente, como se estivesse ligado fisicamente ao computador.

O Amazon EC2 oferece suporte a dois tipos de dispositivo de blocos:

- Volumes de armazenamento de instâncias (dispositivos virtuais cujo hardware subjacente é ligado fisicamente ao computador host da instância)
- Volumes EBS (dispositivos de armazenamento remoto)

Um mapeamento de dispositivos de blocos define os dispositivos de blocos (volumes de armazenamento de instâncias e volumes do EBS) para anexar a uma instância. Você pode especificar um mapeamento de dispositivos de blocos como parte da criação de um AMI para que o mapeamento seja usado por todas as instâncias executadas pela AMI. Como alternativa, você pode especificar um mapeamento de dispositivos de blocos ao executar uma instância, para que o mapeamento cancele o especificado na AMI do qual você iniciou a instância. Observe que todos os volumes de armazenamento de instâncias de NVMe compatíveis com um tipo de instância são automaticamente enumerados e atribuídos a um nome de dispositivo durante a execução da instância. Incluí-los no seu mapeamento de dispositivos de blocos não surtirá nenhum efeito.

Tópicos

- [Entradas do mapeamento de dispositivos de blocos \(p. 1514\)](#)
- [Advertências do armazenamento de instâncias de mapeamento de dispositivos de blocos \(p. 1515\)](#)
- [Exemplo de mapeamento de dispositivos de blocos \(p. 1516\)](#)
- [Como os dispositivos são disponibilizados no sistema operacional \(p. 1516\)](#)

Entradas do mapeamento de dispositivos de blocos

Ao criar um mapeamento de dispositivos de blocos, é preciso especificar as informações a seguir para cada dispositivo de blocos que você precisa associar à instância:

- O nome de dispositivo usado no Amazon EC2. O driver de dispositivo de blocos da instância atribui o nome real do volume ao montar o volume. O nome atribuído pode ser diferente do nome recomendado pelo Amazon EC2. Para obter mais informações, consulte [Nomes de dispositivos em instâncias do Windows. \(p. 1512\)](#).

Para volumes de armazenamento de instâncias, você também especifica as seguintes informações:

- O dispositivo virtual: `ephemeral[0-23]`. Observe que o número e o tamanho de volumes de armazenamento de instâncias disponíveis variam por tipo de instância.

Para volumes de armazenamento de instâncias NVMe, as seguintes informações também se aplicam:

- Esses volumes são automaticamente enumerados e atribuídos a um nome de dispositivo; incluí-los no mapeamento de dispositivos de blocos não surtirá nenhum efeito.

Para volumes do EBS, você também especifica as seguintes informações:

- O ID do snapshot a ser usado para criar o dispositivo de blocos (`snap-xxxxxxxx`). Esse valor é opcional, desde que você especifique um tamanho do volume.
- O tamanho do volume em GiB. O tamanho especificado deve ser maior que ou igual ao tamanho do snapshot especificado.
- Se o volume deve ser excluído no encerramento da instância (`true` ou `false`). O valor padrão é `true` para o volume do dispositivo raiz e `false` para volumes associados. Quando você cria a AMI, o mapeamento de dispositivos de blocos dele herda essa configuração da instância. Quando você executa uma instância, ela herda essa configuração da AMI.
- O tipo de volume, que pode ser `gp2` e `gp3` para SSD de uso geral, `io1` e `io2` para SSD de IOPS provisionadas, `st1` para HDD otimizado para taxa de transferência, `sc1` para HDD a frio ou `standard` para magnético. O valor padrão é `gp2`.
- O número de operações de entrada/saída por segundo (IOPS) que o volume é capaz de suportar. (Usado apenas com volumes `io1` e `io2`.)

Advertências do armazenamento de instâncias de mapeamento de dispositivos de blocos

Há várias advertências a serem consideradas ao executar instâncias com os AMIs que têm volumes de armazenamento de instâncias em seus mapeamentos de dispositivos de blocos.

- Alguns tipos de instância incluem mais volumes de armazenamento de instâncias que outros, e alguns tipos de instância não contêm nenhum volume de armazenamento de instâncias. Se seu tipo de instância for compatível com um volume de armazenamento de instâncias e o AMI tiver mapeamentos para dois volumes de armazenamento de instâncias, a instância será executada com um volume de armazenamento de instâncias.
- Volumes de armazenamento de instâncias só podem ser mapeados no momento da execução. Você não pode interromper uma instância sem volumes de armazenamento de instâncias (como `t2.micro`), alterar a instância para um tipo que suporte os volumes de armazenamento de instâncias e reiniciá-la com volumes de armazenamento de instâncias. No entanto, você pode criar uma AMI com base na instância e executá-la em um tipo de instância que suporte volumes de armazenamento de instâncias e os mapeie para a instância.
- Se você executar uma instância com os volumes de armazenamento de instâncias mapeados e, em seguida, interromper a instância e alterá-la para um tipo de instância com menos volumes de armazenamento de instâncias e reiniciá-la, os mapeamentos do volume de armazenamento de instâncias da execução inicial continuarão a ser exibidos nos metadados da instância. Contudo, somente o número máximo de volumes suportados pelo armazenamento de instâncias para aquele tipo de instância estará disponível.

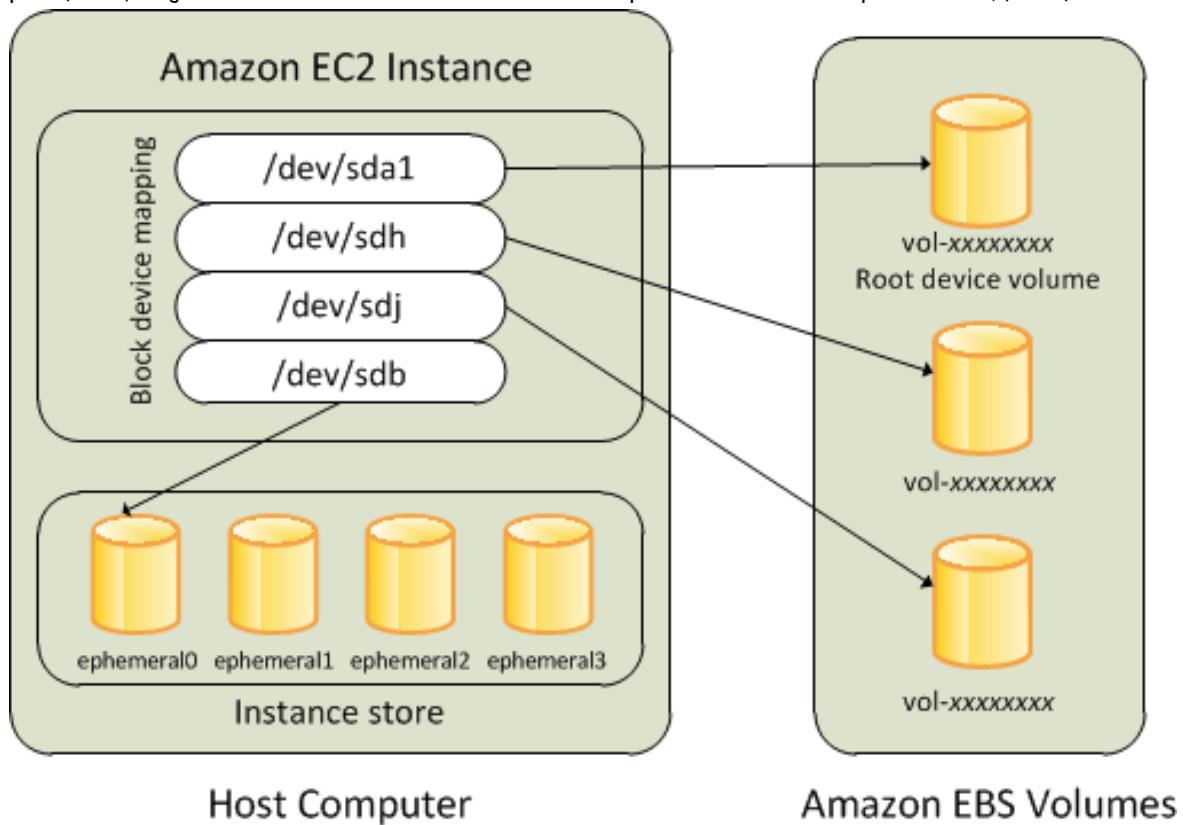
Note

Quando uma instância for interrompida, todos os dados nos volumes do armazenamento de instâncias serão perdidos.

- Dependendo da capacidade de armazenamento das instâncias no momento da execução, as instâncias M3 poderão ignorar os mapeamentos de dispositivos de blocos do armazenamento de instâncias da AMI na execução, a menos que sejam especificadas na execução. Você deve especificar mapeamentos de dispositivos de blocos no armazenamento de instâncias no momento da inicialização, mesmo que a AMI que você está executando tenha os volumes de armazenamento de instâncias mapeados na AMI, de forma a garantir que os volumes de armazenamento das instâncias estejam disponíveis quando a instância é iniciada.

Exemplo de mapeamento de dispositivos de blocos

Essa figura mostra um exemplo de mapeamento de dispositivos de blocos para uma instância com EBS. Isso mapeia /dev/sdb para ephemeral0 e mapeia dois volumes do EBS: uma para /dev/sdh e outro para /dev/sdj. Isso também mostra o volume do EBS que é o volume do dispositivo raiz, /dev/sda1.



Observe que esse exemplo de mapeamento de dispositivos de blocos é utilizado em exemplos de comandos e APIs neste tópico. Você pode encontrar os exemplos de comandos e APIs que criam mapeamentos de dispositivos de blocos em [Especificar um mapeamento de dispositivos de blocos para uma AMI \(p. 1517\)](#) e [Atualizar o mapeamento de dispositivos de blocos ao executar uma instância \(p. 1520\)](#).

Como os dispositivos são disponibilizados no sistema operacional

Nomes de dispositivos, como `/dev/sdh` e `xvdh`, são usados pelo Amazon EC2 para descrever dispositivos de blocos. O mapeamento de dispositivos de blocos é usado pelo Amazon EC2 para especificar os dispositivos de blocos para uma instância do EC2. Após um dispositivo de blocos ser associado a uma instância, ele deverá ser montado pelo sistema operacional antes que você possa

acessar o dispositivo de armazenamento. Quando um dispositivo de blocos é separado de uma instância, ele será desmontado pelo sistema operacional e você não poderá mais acessar o dispositivo de armazenamento.

Com uma instância do Windows, os nomes de dispositivo especificados no mapeamento de dispositivos de blocos são mapeados aos dispositivos de blocos correspondentes quando a instância for inicializada pela primeira vez, e depois o serviço Ec2Config iniciará e montará as unidades. O volume do dispositivo raiz é montado como C:\. Os volumes de armazenamento de instâncias são montados como Z:\, Y:\, etc. Quando um volume do EBS é montado, isso pode acontecer usando qualquer letra de unidade disponível. No entanto, você pode configurar como o serviço EC2Config atribui letras de unidades para os volumes do EBS; para obter mais informações, consulte [Configurar uma instância do Windows usando o serviço EC2Config \(p. 530\)](#).

Mapeamento de dispositivos de blocos da AMI

Cada AMI tem um mapeamento de dispositivos de blocos que especifica os dispositivos de blocos a serem associados a uma instância quando é executada pela AMI. Uma AMI fornecida pelo Amazon inclui somente um dispositivo raiz. Para adicionar mais dispositivos de blocos a uma AMI, você deve criar sua própria AMI.

Tópicos

- [Especificar um mapeamento de dispositivos de blocos para uma AMI \(p. 1517\)](#)
- [Visualizar os volumes do EBS em um mapeamento de dispositivo de blocos da AMI \(p. 1519\)](#)

Especificar um mapeamento de dispositivos de blocos para uma AMI

Há duas maneiras de especificar volumes além do volume do dispositivo raiz ao criar uma AMI. Se você já tiver associado volumes a uma instância em execução antes de criar uma AMI pela instância, o mapeamento de dispositivos de blocos para a AMI incluirá os mesmos volumes. Para volumes do EBS, os dados existentes são salvos em um novo snapshot, e é esse novo snapshot que é especificado no mapeamento de dispositivos de blocos. Para volumes de armazenamento de instâncias, os dados não são preservados.

Para AMIs baseados em EBS, você pode adicionar volumes do EBS e volumes de armazenamento de instâncias usando um mapeamento de dispositivos de blocos. Para AMIs com armazenamento de instâncias, você só poderá adicionar volumes de armazenamento de instâncias ao modificar as entradas de mapeamento de dispositivos de blocos no arquivo manifesto da imagem ao registrar a imagem.

Note

Para instâncias M3, você deve especificar volumes de armazenamento de instâncias no mapeamento de dispositivos de blocos para a instância ao iniciá-los. Quando você executa uma instância M3, os volumes de armazenamento de instâncias especificados no mapeamento de dispositivos de blocos para a AMI poderão ser ignorados se não forem especificados como parte do mapeamento de dispositivos de blocos da instância.

Para adicionar volumes a uma AMI usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione uma instância e escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem).
4. Insira um nome e uma descrição para a imagem.

5. Os volumes de instância aparecem em Volumes de instância (Volumes de instância). Para adicionar outro volume, escolha Add volume (Adicionar volume).
6. Em Volume type (Tipo de volume), escolha o tipo de volume. Para Device (Dispositivo), escolha o nome do dispositivo. Para um volume do EBS, você pode especificar detalhes adicionais, como um snapshot, o tamanho do volume, o tipo de volume, IOPS e estado de criptografia.
7. Escolha Create Image (Criar imagem).

To add volumes to an AMI using the command line (Para adicionar volumes a uma AMI usando a linha de comando)

Use o comando [create-image](#) da AWS CLI para especificar um mapeamento de dispositivos de blocos para uma AMI com EBS. Use o comando [register-image](#) da AWS CLI para especificar um mapeamento de dispositivos de blocos para uma AMI com armazenamento de instâncias.

Especifique o mapeamento de dispositivos de blocos usando o parâmetro `--block-device-mappings`. Os argumentos codificados em JSON podem ser fornecidos diretamente na linha de comando ou por referência a um arquivo:

```
--block-device-mappings [mapping, ...]  
--block-device-mappings [file://mapping.json]
```

Para adicionar um volume de armazenamento de instâncias, use o mapeamento a seguir.

```
{  
    "DeviceName": "xvdb",  
    "VirtualName": "ephemeral0"  
}
```

Para adicionar um volume vazio do gp2 de 100 GiB, use o mapeamento a seguir.

```
{  
    "DeviceName": "xvdg",  
    "Ebs": {  
        "VolumeSize": 100  
    }  
}
```

Para adicionar um volume do EBS com base em um snapshot, use o mapeamento a seguir.

```
{  
    "DeviceName": "xvdh",  
    "Ebs": {  
        "SnapshotId": "snap-xxxxxxxx"  
    }  
}
```

Para omitir um mapeamento de um dispositivo, use o mapeamento a seguir:

```
{  
    "DeviceName": "xvdj",  
    "NoDevice": ""  
}
```

Como alternativa, você pode usar o parâmetro `-BlockDeviceMapping` com os comandos a seguir (AWS Tools for Windows PowerShell):

- [New-EC2Image](#)
- [Register-EC2Image](#)

Visualizar os volumes do EBS em um mapeamento de dispositivo de blocos da AMI

Você pode facilmente enumerar volumes do EBS no mapeamento de dispositivos de blocos para AMI.

Para visualizar os volumes do EBS para uma AMI usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, selecione AMIs.
3. Escolha EBS images (Imagens de EBS) da lista Filter (Filtro) para obter uma lista de AMIs com EBS.
4. Selecione a AMI desejada e examine a guia Details (Detalhes). No mínimo, estarão disponíveis as informações a seguir para o dispositivo raiz:
 - Root Device Type (Tipo de dispositivo raiz (ebs))
 - Root Device Name (Nome do dispositivo raiz) (por exemplo, /dev/sda1)
 - Block Devices (Dispositivos de blocos) (por exemplo, /dev/sda1=snap-1234567890abcdef0:8:true)

Se a AMI tiver sido criada com volumes do EBS adicionais usando um mapeamento de dispositivos de blocos, o campo Block Devices (Dispositivos de blocos) exibirá o mapeamento desses volumes adicionais também. (Essa tela não exibe volumes de armazenamento de instâncias.)

To view the EBS volumes for an AMI using the command line (Para visualizar os volumes do EBS para uma AMI usando a linha de comando)

Use o comando [describe-images](#) (AWS CLI) ou o comando [Get-EC2Image](#) (AWS Tools for Windows PowerShell) para enumerar os volumes do EBS no mapeamento de dispositivos de blocos para uma AMI.

Mapeamento de dispositivos de blocos de instância

Por padrão, uma instância que você inicia inclui todos os dispositivos de armazenamento especificados no mapeamento de dispositivos de blocos da AMI do qual você executou a instância. Você pode especificar alterações ao mapeamento de dispositivos de blocos para uma instância quando ela é iniciada, e essas atualizações se sobrescrevem ou se mesclam com o mapeamento de dispositivos de blocos da AMI.

Limitations

- Para o volume raiz, você só pode modificar o seguinte: tamanho do volume, tipo de volume e o sinalizador Delete on Termination (Excluir ao encerrar).
- Quando modificar um volume do EBS, não será possível reduzir o tamanho. Portanto, você deve especificar um snapshot cujo tamanho seja igual ou maior que o tamanho do snapshot especificado no mapeamento de dispositivos de blocos da AMI.

Tópicos

- [Atualizar o mapeamento de dispositivos de blocos ao executar uma instância \(p. 1520\)](#)
- [Atualizar o mapeamento de dispositivos de blocos de uma instância em execução \(p. 1521\)](#)
- [Visualizar os volumes do EBS em um mapeamento de dispositivos de blocos de instância \(p. 1522\)](#)

- [Visualizar o mapeamento de dispositivos de blocos de instância para volumes de armazenamento de instâncias \(p. 1522\)](#)

Atualizar o mapeamento de dispositivos de blocos ao executar uma instância

Você pode adicionar volumes do EBS e volumes de armazenamento de instâncias a uma instância quando iniciá-la. Observe que atualizar o mapeamento de dispositivos de blocos para uma instância não cria uma alteração permanente no mapeamento de dispositivos de blocos da AMI do qual ela foi executada.

Para adicionar volumes a uma instância usando o console

1. Abra o console do Amazon EC2.
2. No painel, escolha Launch Instance (Executar instância).
3. Na página Choose an Amazon Machine Image (AMI) (Escolha uma imagem de máquina da Amazon), selecione as AMIs a serem usadas e escolha Select (Selecionar).
4. Siga o assistente para preencher as páginas Choose an Instance Type e Configure Instance Details.
5. Na página Add Storage (Adicionar armazenamento), você pode modificar o volume raiz, os volumes do EBS e os volumes de armazenamento de instâncias da seguinte forma:
 - Para alterar o tamanho do volume raiz, localize o volume Root (Raiz) na coluna Type (Tipo) e altere o campo Size (Tamanho).
 - Para excluir um volume do EBS especificado pelo mapeamento de dispositivos de blocos das AMIs usadas para executar a instância, localize o volume e clique no ícone Delete (Excluir).
 - Para adicionar um volume do EBS, escolha Add New Volume (Adicionar novo volume), selecione EBS na lista Type (Tipo) e preencha os campos (Device (Dispositivo), Snapshot, etc.).
 - Para excluir um volume de armazenamento de instâncias especificado pelo mapeamento de dispositivos de blocos da AMI usada para executar a instância, localize o volume e clique no ícone Delete (Excluir).
 - Para adicionar um volume de armazenamento de instâncias, selecione Add New Volume (Adicionar novo volume), Instance Store (Armazenamento de instância) na lista Type (Tipo) e selecione um nome de dispositivo em Device (Dispositivo).
6. Preencha as páginas restantes do assistente e escolha Launch (Executar).

Como adicionar volumes a uma instância usando a AWS CLI

Use o comando `run-instances` da AWS CLI com a opção `--block-device-mappings` para especificar um mapeamento de dispositivos de blocos para uma instância no lançamento.

Por exemplo, vamos supor que a AMI com EBS especifique o seguinte mapeamento de dispositivos de blocos:

- `xvdb=ephemeral0`
- `xvdh=snap-1234567890abcdef0`
- `xvdj=:100`

Para evitar que o `xvdj` seja anexado a uma instância em execução nesta AMI, use o mapeamento a seguir.

```
{  
    "DeviceName": "xvdj",  
    "NoDevice": ""
```

```
}
```

Para aumentar o tamanho de xvdh para 300 GiB, especifique o mapeamento a seguir. Observe que você não precisa especificar o ID do snapshot para xvdh, pois especificar o nome do dispositivo basta para identificar o volume.

```
{
    "DeviceName": "xvdh",
    "Ebs": {
        "VolumeSize": 300
    }
}
```

Para aumentar o tamanho do volume raiz ao iniciar a instância, primeiro chame [describe-images](#) com o ID da AMI para verificar o nome de dispositivo do volume raiz. Por exemplo, "RootDeviceName": "/dev/xvda". Para substituir o tamanho do volume raiz, especifique o nome do dispositivo raiz usado pela AMI e o novo tamanho do volume.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
        "VolumeSize": 100
    }
}
```

Para associar um volume adicional de armazenamento de instâncias, xvdc, especifique o mapeamento a seguir. Se o tipo de instância não oferecer volumes de armazenamento de múltiplas instâncias, esse mapeamento não surtirá efeito. Se a instância for compatível com os volumes de armazenamento de instâncias NVMe, eles serão automaticamente enumerados e receberão um nome de dispositivo NVMe.

```
{
    "DeviceName": "xvdc",
    "VirtualName": "ephemeral1"
}
```

Como adicionar volumes a uma instância usando a AWS Tools for Windows PowerShell

Use o parâmetro `-BlockDeviceMapping` com o comando [New-EC2Instance](#) (AWS Tools for Windows PowerShell)

Atualizar o mapeamento de dispositivos de blocos de uma instância em execução

Você pode usar o comando [modify-instance-attribute](#) da AWS CLI para atualizar o mapeamento de dispositivos de blocos de uma instância em execução. Você não precisa parar a instância para alterar esse atributo.

```
aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings file://mapping.json
```

Por exemplo: para preservar o volume raiz no encerramento da instância, especifique o seguinte no `mapping.json`.

```
[
{
    "DeviceName": "/dev/sda1",
```

```
        "Ebs": {  
            "DeleteOnTermination": false  
        }  
    }  
]
```

Como alternativa, você pode usar o parâmetro `-BlockDeviceMapping` com o comando [Edit-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell).

Visualizar os volumes do EBS em um mapeamento de dispositivos de blocos de instância

Você pode facilmente enumerar volumes do EBS para a instância.

Note

Para instâncias executadas antes do lançamento da API de 31/10/2009, a AWSnão pode exibir o mapeamento de dispositivos de blocos. Você deve separar e reassociar volumes de modo que a AWS possa exibir o mapeamento de dispositivos de blocos.

Para visualizar os volumes do EBS para uma instância usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, escolha Instances (Instâncias).
3. Na caixa de pesquisa, insira Root device type (Tipo de dispositivo raiz) e selecione EBS. Isso exibe uma lista de instâncias baseadas no EBS.
4. Selecione a instância desejada e examine os detalhes exibidos na guia Storage (Armazenamento). No mínimo, estarão disponíveis as informações a seguir para o dispositivo raiz:
 - Root device type (Tipo de dispositivo raiz) (por exemplo, EBS)
 - Root Device Name (Nome do dispositivo raiz) (por exemplo, /dev/xvda)
 - Block devices (Dispositivos de blocos) (por exemplo /dev/xvda, xvdf e xvdj)

Se a instância tiver sido executada com volumes adicionais do EBS usando um mapeamento de dispositivo de bloco, eles aparecerão em Block devices (Dispositivos de bloco). Nenhum dos volumes de armazenamento de instâncias aparece nesta guia.

5. Para exibir informações adicionais sobre um volume do EBS, escolha seu ID de volume para ir para a página de volume. Para obter mais informações, consulte [Visualizar informações sobre um volume do Amazon EBS \(p. 1276\)](#).

To view the EBS volumes for an instance using the command line (Para visualizar os volumes do EBS para uma instância usando a linha de comando)

Use o comando [describe-instances](#) (AWS CLI) ou o comando de [Get-EC2Instance](#) (AWS Tools for Windows PowerShell) para enumerar os volumes do EBS no mapeamento de dispositivos de blocos para uma instância.

Visualizar o mapeamento de dispositivos de blocos de instância para volumes de armazenamento de instâncias

Quando você vir o mapeamento de dispositivos de blocos para sua instância, verá somente os volumes do EBS, não os volumes de armazenamento de instâncias. O método a ser usado para visualizar os volumes de armazenamento de instâncias para a instância depende do tipo de volume.

Volumes de armazenamento de instâncias do NVMe

Você pode usar o pacote de linha de comando do NVMe, [nvme-cli](#), para consultar os volumes de armazenamento de instâncias do NVMe no mapeamento de dispositivos de blocos. Faça download e instale o pacote de sua instância e execute o seguinte comando.

```
[ec2-user ~]$ sudo nvme list
```

Este é um exemplo de saída de uma instância. O texto na coluna Modelo indica se o volume é um volume do EBS ou um volume do armazenamento de instâncias. Neste exemplo, tanto /dev/nvme1n1 como /dev/nvme2n1 são volumes de armazenamento de instâncias.

Node	SN	Model	Namespace
/dev/nvme0n1	vol06afc3f8715b7a597	Amazon Elastic Block Store	1
/dev/nvme1n1	AWS2C1436F5159EB6614	Amazon EC2 NVMe Instance Storage	1
/dev/nvme2n1	AWSB1F4FF0C0A6C281EA	Amazon EC2 NVMe Instance Storage	1
...			

Volumes de armazenamento de instâncias HDD ou SSD

É possível usar os metadados da instância para consultar os volumes de armazenamento de instâncias HDD ou SSD no mapeamento de dispositivos de blocos. Os volumes de armazenamento de instâncias NVMe não estão incluídos.

O URI de base de todas as solicitações de metadados da instância é <http://169.254.169.254/latest/>. Para obter mais informações, consulte [Metadados da instância e dados do usuário \(p. 622\)](#).

Primeiro, conecte-se à instância em execução. Com base na instância, use esta consulta para obter o mapeamento de dispositivos de blocos.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/
```

A resposta inclui o nome dos dispositivo de blocos para a instância. Por exemplo, a saída de uma instância m1.small com armazenamento de instância é semelhante à apresentada a seguir.

```
ami
ephemeral0
root
swap
```

O dispositivo ami é o dispositivo raiz como visto pela instância. Os volumes de armazenamento de instâncias têm o nome ephemeral[0-23]. O dispositivo swap é para o arquivo da página. Se você também tiver mapeado os volumes do EBS, eles serão exibidos como ebs1, ebs2, etc.

Para obter detalhes sobre um dispositivo de blocos individual no mapeamento de dispositivos de blocos, coloque o nome dele na consulta anterior, como mostrado aqui.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

O tipo de instância determina o número de volumes de armazenamento de instâncias que estão disponíveis para a instância. Se o número de volumes de armazenamento de instâncias em um mapeamento de dispositivos de blocos exceder o número de volumes de armazenamento de instâncias disponível para uma instância, os volumes adicionais serão ignorados. Para visualizar os volumes de armazenamento de instâncias da instância, abra o Gerenciamento de Disco do Windows. Para saber a quantidade de volumes de armazenamento de instâncias compatível com cada tipo de instância, consulte [Volumes de armazenamento de instâncias \(p. 1492\)](#).

Mapear discos para volumes na sua instância Windows

Sua instância Windows vem com um volume do EBS que serve como o volume raiz. Se sua instância Windows usar os drivers AWS PV ou Citrix PV, é possível adicionar até 25 volumes, contabilizando um total de 26 volumes. Para obter mais informações, consulte [Limites de volumes de instância \(p. 1507\)](#).

Dependendo do tipo de sua instância, você terá de 0 a 24 volumes de armazenamento de instâncias possíveis disponíveis para a instância. Para usar qualquer um dos volumes de armazenamento de instâncias que estão disponíveis para a instância, você deverá especificá-los ao criar sua AMI ou executar a instância. Você também pode adicionar volumes do EBS ao criar sua AMI ou executar a instância ou anexá-los enquanto a instância estiver em execução. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Windows \(p. 1272\)](#).

Quando você adicionar um volume à sua instância, especifique o nome do dispositivo que o Amazon EC2 usa. Para obter mais informações, consulte [Nomes de dispositivos em instâncias do Windows. \(p. 1512\)](#). AWS As imagens de máquina da Amazon (AMIs) do Windows contêm um conjunto de drivers que são usados pelo Amazon EC2 para mapear o armazenamento de instância e os volumes do EBS aos discos e a letras de unidade do Windows. Se você executar uma instância a partir de uma AMI do Windows que use drivers AWS PV ou Citrix PV, você poderá usar as relações descritas nesta página para mapear os discos do Windows ao seu armazenamento de instâncias e volumes do EBS. Se a AMI da Windows usar drivers Red Hat PV, você pode atualizar sua instância para usar os drivers Citrix. Para obter mais informações, consulte [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#).

Sumário

- [Listar volumes do NVMe \(p. 1524\)](#)
 - [Listar discos de NVMe usando o Gerenciamento de disco \(p. 1525\)](#)
 - [Listar discos do NVMe usando PowerShell \(p. 1525\)](#)
 - [Mapear volumes do EBS de NVMe \(p. 1527\)](#)
- [Listar volumes \(p. 1528\)](#)
 - [Listar discos usando o Gerenciamento de disco \(p. 1528\)](#)
 - [Mapear dispositivos de disco para nomes de dispositivos \(p. 1530\)](#)
 - [Volumes de armazenamento de instâncias \(p. 1530\)](#)
 - [Volumes do EBS \(p. 1530\)](#)
 - [Listar discos usando PowerShell \(p. 1531\)](#)

Listar volumes do NVMe

Você pode encontrar os discos na instância Windows usando Gerenciamento de disco ou Powershell.

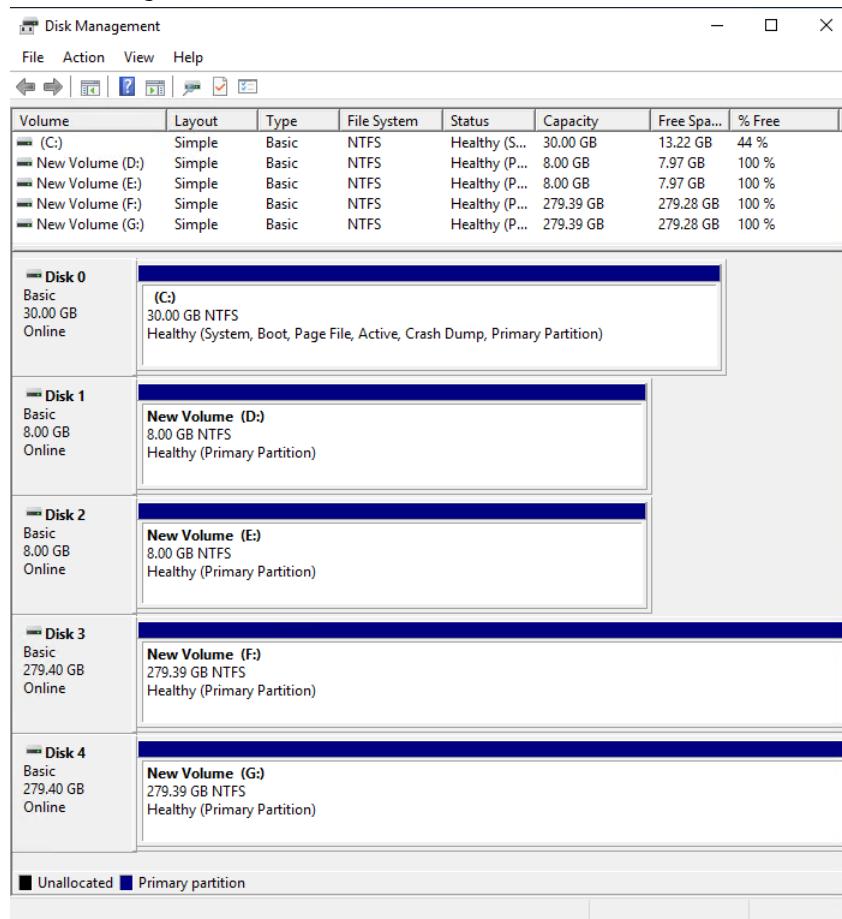
Listar discos de NVMe usando o Gerenciamento de disco

Você pode encontrar os discos na sua instância Windows usando o Gerenciamento de disco do Windows.

Para localizar os discos em sua instância Windows

1. Execute a sessão da sua instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
2. Inicie o utilitário de Gerenciamento de Disco.
3. Revise os discos. O volume raiz é um volume do EBS montado como c:\. Se não houver nenhum outro disco mostrado, você não especificou volumes adicionais quando criou a AMI ou executou a instância.

Veja a seguir um exemplo que mostra os discos disponíveis se você executar uma instância `r5d.4xlarge` com dois volumes adicionais do EBS.



Listar discos do NVMe usando PowerShell

O script do PowerShell a seguir lista cada disco e seu nome de dispositivo e volume correspondentes. Destina-se ao uso com instâncias criadas no [Nitro System \(p. 154\)](#) (Sistema Nitro), que usa volumes do EBS de NVMe e volumes de armazenamento de instâncias.

Conecte-se à sua instância do Windows e execute o seguinte comando para habilitar a execução de script do PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

Copie o seguinte script e salve-o como mapping.ps1 na instância do Windows.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device   = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
    else {
        $Device = "Ephemeral"
        $VolumeName = "Temporary Storage"
    }
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber = (Get-Disk -Path $Path).Number
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber
}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
```

```
$Disk = ( Get-Disk -Path $Path).Number
$EbsVolumeId = GetEBSVolumeId($Path)
$Size =(Get-Disk -Path $Path).Size
$DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
$Device,$VolumeName = GetDeviceName($EbsVolumeId)
$Disk = New-Object PSObject -Property @{
    Disk          = $Disk
    Partitions    = $Partition
    DriveLetter   = $DriveLetter
    EbsVolumeId   = $EbsVolumeId
    Device        = $Device
    VirtualDevice = $VirtualDevice
    VolumeName    = $VolumeName
}
$Report += $Disk
}

$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Execute o script da seguinte forma:

```
PS C:\> .\mapping.ps1
```

Veja a seguir um exemplo de saída para uma instância com um volume raiz, dois volumes do EBS e dois volumes de armazenamento de instâncias.

Disk	Partitions	DriveLetter	EbsVolumeId	Device	VirtualDevice	VolumeName
0	1	C	vol-03683f1d861744bc7	/dev/sdal	root	
1	1	D	vol-082b07051043174b9	xvdb	N/A	
2	1	E	vol-0a4064b39e5f534a2	xvdc	N/A	
3	1	F	AWS-6AAD8C2AEEE1193F0	Ephemeral	N/A	Temporary Storage
4	1	G	AWS-13E7299C2BD031A28	Ephemeral	N/A	Temporary Storage

Se você não tiver fornecido suas credenciais na instância do Windows, o script não poderá obter o ID de volume do EBS e usará N/A na coluna EbsVolumeId.

Mapear volumes do EBS de NVMe

Com instâncias criadas no [sistema Nitro \(p. 154\)](#), os volumes do EBS são expostos como dispositivos NVMe. Você pode usar o comando [Get-Disk](#) para mapear os números de disco do Windows para IDs de volume do EBS. Para obter mais informações, consulte [Identificar o dispositivo EBS \(p. 1439\)](#).

```
PS C:\> Get-Disk
Number Friendly Name Serial Number           HealthStatus
OperationalStatus      Total Size Partition

Style
-----
3   NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.  Healthy      Online
     279.4 GB MBR
4   NVMe Amazo... AWS13E7299C2BD031A28_00000001.  Healthy      Online
     279.4 GB MBR
2   NVMe Amazo... vol0a4064b39e5f534a2_00000001.  Healthy      Online
     8 GB MBR
0   NVMe Amazo... vol03683f1d861744bc7_00000001.  Healthy      Online
     30 GB MBR
1   NVMe Amazo... vol082b07051043174b9_00000001.  Healthy      Online
     8 GB MBR
```

Você também pode executar o comando ebsnvme-id para mapear números de disco do NVMe para IDs de volume do EBS e nomes de dispositivos.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Listar volumes

Você pode encontrar os discos na instância Windows usando Gerenciamento de disco ou Powershell.

Listar discos usando o Gerenciamento de disco

Você pode encontrar os discos na sua instância Windows usando o Gerenciamento de disco do Windows.

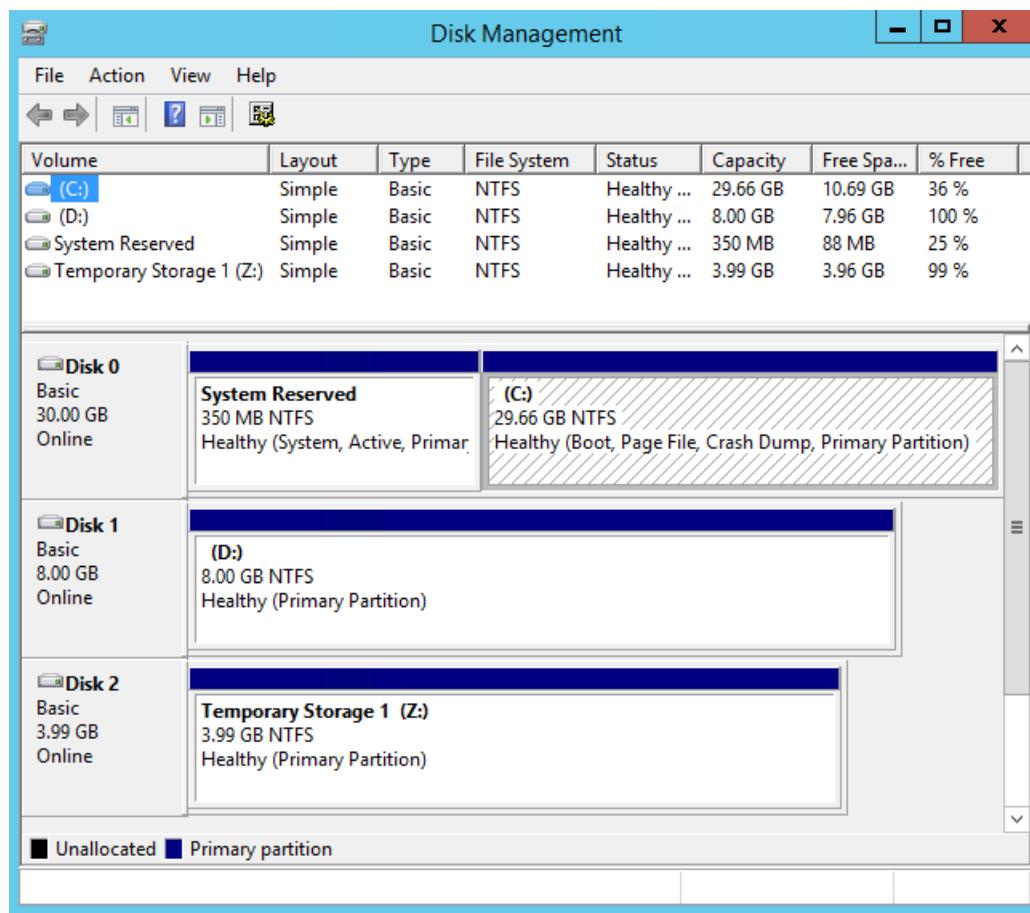
Para localizar os discos em sua instância Windows

1. Execute a sessão da sua instância do Windows usando o Desktop Remoto. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
2. Inicie o utilitário de Gerenciamento de Disco.

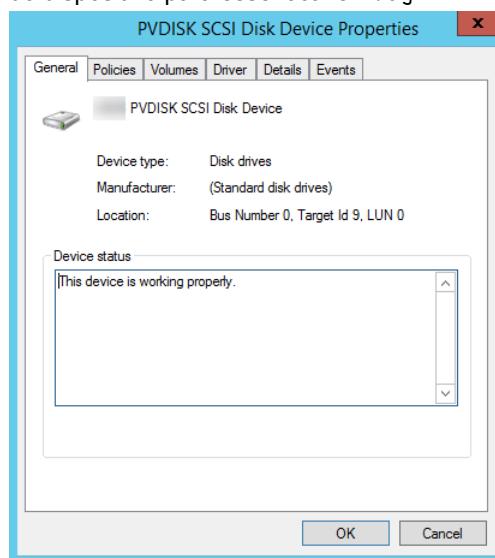
No Windows Server 2012 e posterior, na barra de ferramentas, clique com o botão direito do mouse no logo do Windows e escolha Disk Management (Gerenciamento de disco). No Windows Server 2008, escolha Iniciar, Ferramentas administrativas, Gerenciamento do computador, Disk Management.

3. Revise os discos. O volume raiz é um volume do EBS montado como C:\. Se não houver nenhum outro disco mostrado, você não especificou volumes adicionais quando criou a AMI ou executou a instância.

Veja a seguir um exemplo que mostra os discos que estão disponíveis se você executar uma instância m3.medium com um volume de armazenamento de instâncias (disco 2) e um volume do EBS adicional (disco 1).



- Clique com o botão direito no painel cinza identificado como Disco 1 e selecione Properties (Propriedades). Observe o valor de Location (Local) e procure-o nas tabelas em [Mapear dispositivos de disco para nomes de dispositivos \(p. 1530\)](#). Por exemplo, o seguinte disco tem o Número de barramento de local 0, ID de destino 9, LUN 0. De acordo com a tabela de volumes do EBS, o nome do dispositivo para esse local é xvdfj.



Mapear dispositivos de disco para nomes de dispositivos

O driver de dispositivo de blocos da instância distribui os nomes de volume reais ao montar volumes.

Mapeamentos

- [Volumes de armazenamento de instâncias \(p. 1530\)](#)
- [Volumes do EBS \(p. 1530\)](#)

Volumes de armazenamento de instâncias

A tabela a seguir descreve como os drivers Citrix PV e AWS PV mapeiam volumes de armazenamento de instâncias não NVMe a volumes do Windows. O número de volumes de armazenamento de instâncias disponíveis é determinado pelo tipo de instância. Para obter mais informações, consulte [Volumes de armazenamento de instâncias \(p. 1492\)](#).

Local	Nome do dispositivo
Barramento número 0, ID de destino 78, LUN 0	xvdca
Barramento número 0, ID de destino 79, LUN 0	xvdcb
Barramento número 0, ID de destino 80, LUN 0	xvdcc
Barramento número 0, ID de destino 81, LUN 0	xvdcd
Barramento número 0, ID de destino 82, LUN 0	xvdce
Barramento número 0, ID de destino 83, LUN 0	xvdcf
Barramento número 0, ID de destino 84, LUN 0	xvdcg
Barramento número 0, ID de destino 85, LUN 0	xvdch
Barramento número 0, ID de destino 86, LUN 0	xvdci
Barramento número 0, ID de destino 87, LUN 0	xvdcj
Barramento número 0, ID de destino 88, LUN 0	xvdck
Barramento número 0, ID de destino 89, LUN 0	xvdcl

Volumes do EBS

A tabela a seguir descreve como os drivers Citrix PV e AWS PV mapeiam volumes do EBS não NVME a volumes do Windows.

Local	Nome do dispositivo
Barramento número 0, ID de destino 0, LUN 0	/dev/sda1
Barramento número 0, ID de destino 1, LUN 0	xvdb
Barramento número 0, ID de destino 2, LUN 0	xvdc
Barramento número 0, ID de destino 3, LUN 0	xvdd
Barramento número 0, ID de destino 4, LUN 0	xvde

Local	Nome do dispositivo
Barramento número 0, ID de destino 5, LUN 0	xvdf
Barramento número 0, ID de destino 6, LUN 0	xvdg
Barramento número 0, ID de destino 7, LUN 0	xvdh
Barramento número 0, ID de destino 8, LUN 0	xvdi
Barramento número 0, ID de destino 9, LUN 0	xvdj
Barramento número 0, ID de destino 10, LUN 0	xvdk
Barramento número 0, ID de destino 11, LUN 0	xndl
Barramento número 0, ID de destino 12, LUN 0	xvdm
Barramento número 0, ID de destino 13, LUN 0	xvdn
Barramento número 0, ID de destino 14, LUN 0	xvdo
Barramento número 0, ID de destino 15, LUN 0	xvdp
Barramento número 0, ID de destino 16, LUN 0	xvdq
Barramento número 0, ID de destino 17, LUN 0	xvdr
Barramento número 0, ID de destino 18, LUN 0	xvds
Barramento número 0, ID de destino 19, LUN 0	xvdt
Barramento número 0, ID de destino 20, LUN 0	xvdu
Barramento número 0, ID de destino 21, LUN 0	xvdv
Barramento número 0, ID de destino 22, LUN 0	xvdw
Barramento número 0, ID de destino 23, LUN 0	xvdx
Barramento número 0, ID de destino 24, LUN 0	xvdy
Barramento número 0, ID de destino 25, LUN 0	xvdz

Listar discos usando PowerShell

O script do PowerShell a seguir lista cada disco e seu nome de dispositivo e volume correspondentes.

Requisitos e limitações

- Requer o Windows Server 2012 ou posterior.
- Requer credenciais para obter o ID de volume do EBS. Você pode configurar um perfil usando o Tools for PowerShell, ou anexar uma função do IAM à instância.
- Não suporta volumes NVMe.
- Não suporta discos dinâmicos.

Conecte-se à sua instância do Windows e execute o seguinte comando para habilitar a execução de script do PowerShell.

```
Set-ExecutionPolicy RemoteSigned
```

Copie o seguinte script e salve-o como mapping.ps1 na instância do Windows.

```
# List the disks

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function Convert-SCSITargetIdToDeviceName {
    param([int]$SCSITargetId)
    If ($SCSITargetId -eq 0) {
        return "sdal"
    }
    $deviceName = "xvd"
    If ($SCSITargetId -gt 25) {
        $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
    }
    $deviceName += [char](0x61 + $SCSITargetId % 26)
    return $deviceName
}

Try {
    $InstanceId = Get-EC2InstanceMetadata "meta-data/instance-id"
    $AZ = Get-EC2InstanceMetadata "meta-data/placement/availability-zone"
    $Region = $AZ.Remove($AZ.Length - 1)
    $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
    $InstanceId).Instances.BlockDeviceMappings
    $VirtualDeviceMap = @{}
    (Get-EC2InstanceMetadata "meta-data/block-device-mapping").Split("`n") | ForEach-Object {
        $VirtualDevice = $_
        $BlockDeviceName = Get-EC2InstanceMetadata "meta-data/block-device-mapping/
$VirtualDevice"
        $VirtualDeviceMap[$BlockDeviceName] = $VirtualDevice
        $VirtualDeviceMap[$VirtualDevice] = $BlockDeviceName
    }
}
Catch {
    Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys." -ForegroundColor Yellow
}

Get-disk | ForEach-Object {
    $DriveLetter = $null
    $VolumeName = $null

    $DiskDrive = $_
    $Disk = $_.Number
    $Partitions = $_.NumberOfPartitions
    $EbsVolumeID = $_.SerialNumber -replace "[^ ]*\$" -replace "vol", "vol-"
    Get-Partition -DiskId $_.Path | ForEach-Object {
        if ($_.DriveLetter -ne "") {
            $DriveLetter = $_.DriveLetter
            $VolumeName = (Get-PSDrive | Where-Object {$_ .Name -eq $DriveLetter}).Description
        }
    }

    If ($DiskDrive.path -like "*PROD_PVDISK*") {
        $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -
Class Win32_Diskdrive | Where-Object {$_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
$DiskDrive.Number)}).SCSITargetId)
        $BlockDeviceName = "/dev/" + $BlockDeviceName
    }
}
```

```

$BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*"+$_.DeviceName+"*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
    $VirtualDevice = If ($VirtualDeviceMap.ContainsKey($BlockDeviceName))
    { $VirtualDeviceMap[$BlockDeviceName] } Else { $null }
}
ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = Get-EC2InstanceMetadata "meta-data/block-device-mapping/
ephemeral$((Get-WmiObject -Class Win32_Diskdrive | Where-Object {$_.DeviceID -eq ("\\.\\"$PhysicalDrive"+$DiskDrive.Number) }).SCSIPort - 2)"
    $BlockDevice = $null
    $VirtualDevice = If ($VirtualDeviceMap.ContainsKey($BlockDeviceName))
    { $VirtualDeviceMap[$BlockDeviceName] } Else { $null }
}
ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object {$_.ebs.VolumeId -eq $EbsVolumeID}).DeviceName
    $VirtualDevice = $null
}
Else {
    $BlockDeviceName = $null
    $BlockDevice = $null
    $VirtualDevice = $null
}
New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeID   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else { $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
}
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions, DriveLetter,
EbsVolumeID, Device, VirtualDevice, VolumeName

```

Execute o script da seguinte forma:

```
PS C:\> .\mapping.ps1
```

A seguir está um exemplo de saída.

Disk	Partitions	DriveLetter	EbsVolumeId	Device	VirtualDevice	VolumeName
0	1	Z	N/A	xvdca	ephemeral0	N/A
1	1	Y	N/A	xvdcb	ephemeral1	N/A
2	2	C	vol-0064aexamplec838a	/dev/sdal	root	Windows
3	1	D	vol-02256example8a4a3	xvdf	ebs2	N/A

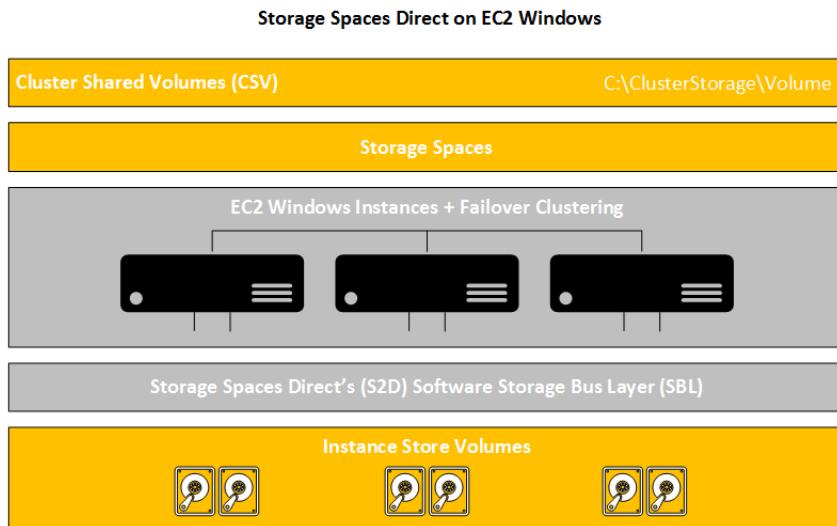
Se você não tiver fornecido suas credenciais na instância do Windows, o script não poderá obter o ID de volume do EBS e usará N/A na coluna EbsVolumeId.

Tutorial: Implantar o Storage Spaces Direct (S2D) no Amazon EC2

O Storage Spaces Direct (S2D) é uma arquitetura de armazenamento altamente dimensionável definida por software, que permite que os usuários agrupem armazenamento local com recursos no Windows

Server 2016. O S2D é uma alternativa às matrizes SAN ou NAS tradicionais. Ele usa recursos e ferramentas integrados do Windows para configurar armazenamento altamente disponível que cruza vários nós em um cluster. Para obter mais informações, visite [Storage Spaces Direct](#) na documentação da Microsoft.

O diagrama a seguir mostra a arquitetura do S2D no Amazon EC2 para Windows.



Nível de habilidade

Um conhecimento básico do Windows Server, bem como de computação de como criar e gerenciar instâncias do Amazon EC2 para Windows ingressadas no domínio em uma VPC é necessário. Conhecimento do AWS Tools for Windows PowerShell e do Clustering de Failover do Windows é útil, mas não é necessário.

O que você vai aprender neste tutorial

- Provisionar um cluster de armazenamento altamente disponível usando o [Storage Spaces Direct \(S2D\)](#).
 - Provisionar um volume compartilhado clusterizado (CSV - cluster-shared volume) em seu cluster.

Antes de começar

- Se ainda não tiver feito isso, abra <https://aws.amazon.com/> e crie uma conta da AWS.
 - Crie uma nuvem privada virtual (VPC) com uma sub-rede pública e duas sub-redes privadas para suas instâncias. Uma terceira sub-rede privada deve ser configurada para o AWS Directory Service.
 - Selecione uma das últimas Imagens de máquina da Amazon (AMI) para o Windows Server 2016. Você pode usar essa AMI como está ou usá-la como base para sua própria AMI personalizada. A AWS recomenda o uso da AMI pública mais recente do EC2 Windows Server 2016.
 - Crie um diretório do AWS Directory Service. Isso não é mais um requisito para habilitar o recurso de cluster de failover no Windows Server 2016. No entanto, este tutorial pressupõe que as instâncias serão associadas a um domínio do Active Directory, no EC2 ou no Active Directory gerenciado pela AWS. Para obter mais informações, consulte [Getting Started with AWS Directory Service](#) (Conceitos básicos sobre o AWS Directory Service) no AWS Directory Service Administration Guide (Guia de administração do AWS Directory Service).
 - Instale e configure o AWS Tools for Windows PowerShell em seu computador. Para obter mais informações, consulte o [Guia do usuário do AWS Tools for Windows PowerShell](#).

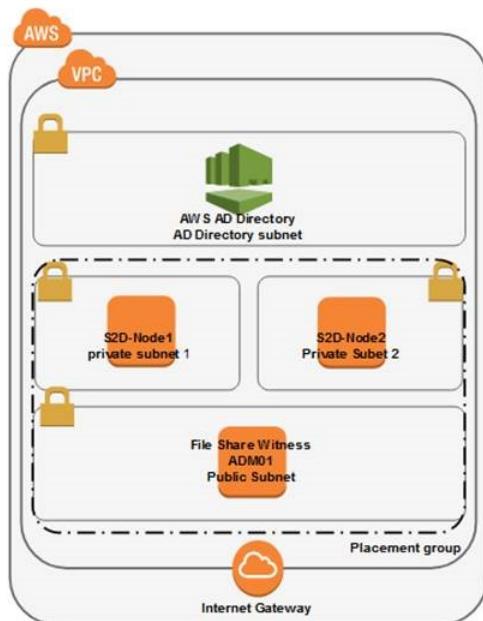
Considerações importantes

- A interrupção de instâncias com [volumes de armazenamento de instâncias \(p. 1490\)](#) poderá causar a perda de dados se não for feito um backup dos dados ou se eles não forem replicados. Os dados em um armazenamento de instâncias persistem apenas durante a vida útil da instância associada. Se uma instância for reiniciada (intencionalmente ou acidentalmente), dados no armazenamento de instância persistirão. Contudo, os dados no armazenamento de instâncias serão perdidos nas seguintes circunstâncias:
 - Há uma falha na unidade de disco subjacente.
 - A instância é interrompida.
 - A instância é encerrada.
- A interrupção de muitas instâncias em um cluster poderá causar a perda de dados se não for feito um backup dos dados ou se eles não forem replicados. Quando você usa o S2D na AWS, como com qualquer cluster, a perda de mais nós do que a tolerância a falhas permite resultará em perda de dados. Um dos maiores riscos de qualquer cluster é perder todos os nós. A redundância de clusters protege contra falhas em uma única instância (ou mais, se a tolerância a falhas oferecer suporte a ela). No entanto, você poderá perder dados se o número de instâncias com unidades de disco com falha em um cluster exceder a tolerância a falhas. Você também pode perder dados se o número de instâncias interrompidas ou encerradas exceder a tolerância a falhas. Para reduzir o risco, limite o número de pessoas ou sistemas que podem interromper ou encerrar instâncias no cluster. Para reduzir o risco de encerrar instâncias do nó de cluster, [habilite a proteção contra encerramento \(p. 476\)](#) nessas instâncias. Você também pode configurar as [IAM policies](#) (Políticas do IAM) para permitir que os usuários somente reiniciem os nós no console da AWS Management Console, mas não os interrompa.
- O S2D não protege contra falhas de rede ou do datacenter que afetem o cluster inteiro. Para reduzir o risco, considere o uso de hosts dedicados para garantir que as instâncias não sejam colocadas no mesmo rack.

Tarefas

- [Etapa 1: Executar e ingressar instâncias no domínio \(p. 1536\)](#)
- [Etapa 2: Instalar e configurar os pré-requisitos de instâncias \(p. 1538\)](#)
- [Etapa 3: Criar cluster de failover \(p. 1540\)](#)
- [Etapa 4: Habilitar o S2D \(p. 1540\)](#)
- [Etapa 5: Provisionar o armazenamento \(p. 1541\)](#)
- [Etapa 6: Rever os recursos do S2D \(p. 1541\)](#)
- [Etapa 7: Limpeza \(p. 1542\)](#)
- [Recursos adicionais \(p. 1543\)](#)

O diagrama a seguir mostra a arquitetura de um cluster de dois nós do EC2 para Windows S2D usando uma testemunha de compartilhamento de arquivos hospedada em uma máquina bastion existente na AWS.



Etapa 1: Executar e ingressar instâncias no domínio

Todas as instâncias do Nitro oferecem suporte ao Storage Spaces Direct usando EBS e/ou NVMe. Todas as instâncias atuais baseadas na geração Xen oferecem suporte ao Storage Spaces Direct com instalação do driver AWS PV 8.2.3 e posterior. A melhor performance de armazenamento pode ser obtida usando instâncias I3 porque elas fornecem armazenamento de instância local com NVMe e alta performance de rede. A configuração do S2D no Amazon EC2 exige um cluster de um mínimo duas e um máximo de 16 instâncias. Essas instâncias devem ter pelo menos dois dispositivos NVMe com conexões de rede de alta performance entre os nós e executar o Windows Server 2016. Para obter mais informações, visite [Requisitos de hardware do Storage Spaces Direct](#) na documentação da Microsoft.

Recomendamos o tamanho da instância I3 porque ele atende aos [Requisitos de hardware do S2D](#) e inclui os dispositivos de armazenamento de instâncias maiores e mais rápidos disponíveis. Também inclui redes avançadas, o que maximiza os recursos disponíveis para S2D por instância. Você pode usar os tipos de instância M5D e R5D, que têm pelo menos 2 discos NVMe, mas os discos de armazenamento de instâncias locais serão usados como discos de cache para o cluster do Storage Spaces Direct e pelo menos 2 volumes do EBS deverão ser adicionados a cada instância para fornecer armazenamento de capacidade.

Recomendamos executar três instâncias para aproveitar o espelhamento de três vias [Tolerância a falhas do S2D](#), o que permite realizar a manutenção em um único nó, mantendo a tolerância a falhas no cluster se uma testemunha, como uma testemunha de compartilhamento de arquivo, estiver configurada. Você também pode usar espelhamento bidirecional com duas instâncias como uma solução mais barata, mas uma testemunha será necessária, e a alta disponibilidade não será mantida durante a manutenção em um nó de cluster.

Implantaremos uma arquitetura de cluster de dois nós usando uma testemunha de compartilhamento de arquivo hospedada em uma máquina bastion que atua como nossa estação de trabalho de administração. Cada nó do cluster deve ser implantado em uma sub-rede diferente. Essa arquitetura será implantada em uma única zona de disponibilidade, pois, atualmente, a Microsoft não oferece suporte a cluster estendido com o Storage Spaces Direct. No entanto, a performance de uma única zona de disponibilidade e de várias zonas de disponibilidade é exatamente o mesmo como resultado de nosso design de latência muito baixa e largura de banda alta para zonas de disponibilidade.

Para executar instâncias de seu cluster

1. Usando o console do Amazon EC2 ou o cmdlet [New-EC2Instance](#), execute duas instâncias `i3.8xlarge` para criar o cluster, e uma instância `t2.medium` como uma estação de trabalho de administração para hospedar a testemunha de compartilhamento de arquivo. Use uma sub-rede diferente para cada instância. Para seguir uma lógica de atribuição de IP, defina o endereço IP privado primário na hora da criação. Nesse caso, você precisará definir um endereço IP privado secundário para cada nó de cluster porque o IP secundário será atribuído ao VIP do cluster mais tarde.

Para criar cada instância com o PowerShell, use o comando [New-EC2Instance](#).

```
New-EC2Instance -ImageId ami-c49c0dac -MinCount 1 -MaxCount 1 -KeyName myPSKeyPair -  
SecurityGroupId mySGID -InstanceType i3.8xlarge -SubnetId mysubnetID
```

Para criar um diretório do AWS AD com o PowerShell, use o comando [New-DSMicrosoftAD](#) (ou, consulte [Criar seu diretório do Microsoft AD gerenciado pela AWS na AWS](#)).

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd -  
Description "AWS DS Managed" - VpcSettings_VpcId vpc-xxxxxxxx -VpcSettings_SubnetId  
subnet-xxxxxxxx, subnet-xxxxxxxx
```

Usamos a seguinte configuração da interface de rede S2D-node1:

▼ Network interfaces ⓘ		Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface ▾			subnet-9850a3fe	172.16.1.199	172.16.1.200	Add IP
						172.16.1.201	Add IP

Note

Cada função implantada neste cluster, como uma instância de cluster de failover do SQL ou servidor de arquivos, exigirá endereços IP secundários adicionais em cada nó. A exceção é a função de Expansão do servidor de arquivos, que não exige um ponto de acesso.

Usamos a seguinte configuração:

Nome do NetBIOS do servidor	Endereço IP	Sub-redes
S2D-Node1	172.16.1.199 (primário) 172.16.1.200 (secundário que será usado para o VIP do cluster) 172.16.1.201 (secundário que será usado mais tarde para uma função, como a FCI do SQL)	AZ1 (por exemplo, eu-west-1a) – sub-rede privada 1

Nome do NetBIOS do servidor	Endereço IP	Sub-redes
S2D-Node2	172.16.3.199 (primário) 172.16.3.200 (secundário que será usado para o VIP do cluster) 172.16.3.201 (secundário que será usado mais tarde para uma função, como a FCI do SQL)	AZ1 (por exemplo, eu-west-1a) – sub-rede privada 2
ADM01	Não especificado	AZ1 (por exemplo, eu-west-1a) – sub-rede pública

2. Você pode usar ingresso no domínio contínuo na hora da criação para ingressar instâncias no domínio. Para ingressá-las no domínio depois que forem iniciadas, use o comando [Add-Computer](#). Recomendamos o uso do AWS Systems Manager e do [AWS Directory Service](#) para inserir com facilidade instâncias do EC2 em um domínio.

As etapas do restante deste tutorial exigem a execução com uma conta de domínio com privilégios administrativos locais em cada instância. Renomeie as instâncias conforme desejado antes de passar para a configuração. Verifique se seus grupos de segurança e firewalls do Windows estão configurados corretamente para permitir a conexão remota ao PowerShell e a comunicação de cluster nesses nós.

Etapa 2: Instalar e configurar os pré-requisitos de instâncias

O S2D exige os recursos de Serviços de arquivos e de Cluster de failover do Windows e pelo menos uma interface de rede de 10 Gbps. Recomendamos configurar o SMB para usar [SMB Multicanal](#), com contagens de conexões de clientes RSS que correspondam à contagem de filas RSS do adaptador de redes avançadas.

As etapas a seguir serão realizadas na instância bastion ADM01.

Para instalar os recursos necessários do Windows

- Instale os recursos de Serviços de arquivos e de Cluster de failover do Windows com as ferramentas de gerenciamento nos nós de cluster. Instale apenas as ferramentas de gerenciamento de failover na ADM01.

Note

Altere "S2D-Node1" e "S2D-Node2" para refletirem os nomes dos computadores que você definir para as duas instâncias. Caso contrário, os valores não serão alterados.

```
$nodes = "S2D-Node1", "S2D-Node2"
foreach ($node in $nodes) {
    Install-WindowsFeature -ComputerName $node -Name File-Services, Failover-Clustering
    -IncludeManagementTools
}
```

```
Install-WindowsFeature -Name RSAT-Clustering
```

Para configurar as redes

1. Habilite o multicanal e defina a contagem de conexões RSS.

```
foreach ($node in $nodes) {
    Invoke-Command -ComputerName $node -ScriptBlock {
        [int]$RssQCount = (Get-NetAdapterAdvancedProperty | Where DisplayName -like "Maximum Number of RSS Queues").RegistryValue | Select -First 1
        $Params = @{
            EnableMultiChannel          = $true;
            ConnectionCountPerRssNetworkInterface = $RssQCount;
            Confirm                      = $false;
        }
        Set-SmbClientConfiguration @Params
    }
}
```

2. Configure o RSS.

```
foreach ($node in $nodes) {
    Invoke-Command -ComputerName $node -ScriptBlock {
        Get-WmiObject -class Win32_processor | ft systemname, Name, DeviceID,
        NumberOfCores, NumberOfLogicalProcessors
        $maxvcpu = (Get-WmiObject -class Win32_processor).NumberOfLogicalProcessors
        Get-NetAdapter | Set-NetAdapterRss -BaseProcessorNumber 2 -MaxProcessors
        $maxvcpu
    }
}
```

Note

Você verá uma mensagem de desconexão quando executar esse comando porque o adaptador de rede é reiniciado depois da configuração do RSS.

O Receive Side Scaling (RSS) é uma tecnologia muito importante em redes no Windows. O RSS garante que o tráfego de rede de entrada seja distribuído entre os processadores disponíveis no servidor para processamento. Se o RSS não for usado, o processamento de rede será vinculado a um processador, que é limitado a aproximadamente 4 GBps. Atualmente, cada NIC, por padrão, permite o RSS, mas a configuração não é otimizada. Cada NIC é configurado, por padrão, com "Processador base" 0, o que significa que ele iniciará o processamento no processador 0 junto com as outras NICs. Para configurar o RSS de forma ideal, comece no processador 1 para não interferir com o padrão de aterrissagem de processos no processador 0.

3. Aumente o valor de tempo limite de E/S do espaço de armazenamento para 30 segundos (recomendado quando configurado em um cluster convidado).

```
foreach ($node in $nodes) {
    Invoke-Command -ComputerName $node -ScriptBlock {
        Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\spaceport
        \Parameters -Name HwTimeout -Value 0x00007530 -Verbose
    }
}
```

4. Reinicie todos os nós para aplicar todas as alterações.

```
Restart-Computer -ComputerName $nodes -Wait -For Wmi -Force
```

Etapa 3: Criar cluster de failover

O S2D é um recurso que é habilitado em um cluster de failover. Depois de habilitar o S2D em um cluster de failover, ele assume o controle do armazenamento local de cada nó no cluster. Por esse motivo, recomendamos instalar um cluster sem armazenamento na hora da criação e, em seguida, habilitar o S2D.

Ao criar um cluster na AWS, você deve atribuir endereços IP estáticos em cada sub-rede da qual um nó é implantado. No console, eles devem ser definidos como endereços IP privados secundários em cada nó. Para este tutorial, configuramos 172.16.1.200 e 172.16.3.200 após a implantação de cada nó.

Você pode verificar e revisar a configuração do cluster com o comando incorporado [Test-Cluster](#).

Testar e verificar a configuração do cluster

1. Execute o comando [Test-Cluster](#) com os testes Storage Spaces Direct, Inventory, Network e System Configuration.

```
$report = Test-Cluster -Node $nodes -Include 'Storage Spaces Direct', 'Inventory', 'Network', 'System Configuration'
```

2. Reveja os resultados dos testes.

```
$reportFilePath = $report.FullName  
Start-Process $reportFilePath
```

3. Crie o cluster usando [New-Cluster](#). Aos IPs virtuais deve ser atribuído um endereço IP privado secundário no Console da AWS Management Console para cada nó respectivo.

```
$vips = "172.16.1.200", "172.16.3.200"  
New-Cluster -Name S2D -Node $nodes -StaticAddress $vips -NoStorage
```

4. Configure uma testemunha de compartilhamento de arquivo.

```
New-Item -ItemType Directory -Path c:\Share\Witness  
[string]$DomainName = (Get-WmiObject win32_computersystem).domain  
New-SmbShare -Name fsw -Path c:\Share\Witness -FullAccess ($DomainName + "\Domain Computers")  
Set-ClusterQuorum -Cluster S2D -FileShareWitness \\$env:COMPUTERNAME\fsw
```

Etapa 4: Habilitar o S2D

Quando o cluster estiver pronto, habilite o S2D em um dos nós usando [Enable-ClusterS2D](#) da seguinte forma. Como temos apenas um tipo de disco em nossa configuração (NVMe local), não vamos usar nenhum disco como um disco de cache.

1. Habilite o S2D em tipos de instância i3 usando o comando [Enable-ClusterS2D](#).

```
Enable-ClusterS2D -PoolFriendlyName S2DPool -Confirm:$false -SkipEligibilityChecks:$true -CimSession $nodes[0]
```

2. Se estiver usando tipos de instância m5d ou r5d com NVMe e EBS, use os discos NVMe como discos de cache. O comando deve ser semelhante a este:

```
Enable-ClusterS2D -PoolFriendlyName S2DPool -CacheDeviceModel "Amazon EC2 NVMe" -Confirm:$false -SkipEligibilityChecks:$true -CimSession $nodes[0]
```

Etapa 5: Provisionar o armazenamento

Para provisionar o armazenamento, crie um grupo de armazenamento e, em seguida, crie volumes nesse grupo. Para simplificar, por padrão, o comando [Enable-ClusterS2D](#) cria um grupo usando todos os discos disponíveis no cluster. Com esse comando configuramos o nome do grupo de armazenamento como "S2D Pool" (Grupo S2D).

Depois de criados os volumes, eles se tornam acessíveis a cada nó no cluster. Os volumes podem então ser atribuídos a uma função específica no cluster, como uma função de servidor de arquivos, ou podem ser atribuídos como [volumes compartilhados de cluster](#) (CSV). Um CSV é acessível para o cluster inteiro, o que significa que cada nó no cluster pode gravar e ler nesse volume.

Para melhorar a performance, recomendamos usar provisionamento fixo e um sistema de arquivos ReFS para CSV. O tamanho do setor depende do tipo das workloads que serão implantadas no cluster. Para obter mais informações sobre o tamanho do setor, consulte [Recomendações de tamanho de clusters para ReFS e NTFS](#). Para melhorar a performance de leitura local, recomendamos alinhar o CSV com o nó que hospeda sua aplicação ou workload. Você pode ter vários CSVs e várias aplicações distribuídas entre os nós.

Criar um volume compartilhado de cluster (CSV)

- Use o comando [New-Volume](#) para criar um novo CSV de 1 TB.

```
$Params = @{
    FriendlyName      = 'CSV1';
    FileSystem        = 'CSVFS_ReFS';
    StoragePoolFriendlyName = 'S2DPool';
    Size              = 1TB;
    AllocationUnitSize = 65536;
    ProvisioningType   = 'Fixed';
    CimSession         = $nodes[0];
}
New-Volume @Params
```

Etapa 6: Rever os recursos do S2D

Os recursos do S2D que você configurou são exibidos no Gerenciador de cluster de failover.

Para visualizar seu CSV

1. Abra o Gerenciador de Servidores.
2. Escolha Tools (Ferramentas), Failover Cluster Manager (Gerenciador de cluster de failover).
3. Expanda o nome do cluster, expanda Storage (Armazenamento) e escolha Disks (Discos).

O nome amigável, a capacidade, o nó que hospeda o CSV e outros dados são listados. Para obter mais informações sobre o gerenciamento de CSVs, consulte [Usar volumes compartilhados de cluster em um cluster de failover](#).

Para sintetizar uma carga no CSV

Use uma ferramenta como o [Utilitário Diskspd](#). Conecte-se a um dos nós de cluster com RDP e execute o seguinte com a ferramenta Diskspd.

```
$mycsv = (gci C:\ClusterStorage\ | select -First 1).fullname
```

```
.\diskspd.exe -d60 -b4k -o1024 -t32 -L -Sh -r -w50 -W60 -c100G $mycsv\test.dat
```

Para visualizar a performance do armazenamento do S2D do cluster

Use o comando [Get-StorageHealthReport](#) para visualizar a performance do cluster em um dos nós do cluster.

1. Abra uma nova janela do PowerShell e inicie sua workload sintetizada.
2. Nas janelas do PowerShell original, execute [Get-StorageSubSystem *cluster*](#) | [Get-StorageHealthReport](#) para ver os resultados da performance do subsistema de armazenamento enquanto a workload está em execução.

```
PS C:\> Get-StorageSubSystem *cluster* | Get-StorageHealthReport

CPUUsageAverage          : 60.44 %
CapacityPhysicalPooledAvailable : 9.82 GB
CapacityPhysicalPooledTotal   : 13.82 TB
CapacityPhysicalTotal       : 13.82 TB
CapacityPhysicalUnpooled    : 0 B
CapacityVolumesAvailable   : 1.89 TB
CapacityVolumesTotal        : 2 TB
IOLatencyAverage           : 257.56 ms
IOLatencyRead              : 255.87 ms
IOLatencyWrite              : 259.25 ms
IOPSRead                   : 64327.37 /S
IOPSTotal                  : 128582.85 /S
IOPSSWrite                 : 64255.49 /S
IOThroughputRead           : 251.28 MB/S
IOThroughputTotal           : 502.28 MB/S
IOThroughputWrite           : 251 MB/S
MemoryAvailable             : 477.77 GB
MemoryTotal                 : 488 GB
```

Etapa 7: Limpeza

Se você seguiu o tutorial para criar um cluster de armazenamento altamente disponível usando S2D no EC2 para Windows, você terá criado um cluster do Storage Spaces Direct de duas instâncias em um servidor bastion, que também serve como uma testemunha de compartilhamento de arquivo para o cluster. Você é cobrado por cada hora ou hora parcial em que as instâncias são mantidas em execução. Quando você não precisar mais do cluster, use o console do EC2 ou o [AWS Tools for Windows](#) para excluir os recursos criados para este projeto. Faça isso excluindo o cluster a partir do mmc de gerenciamento de cluster de failover, encerrando as instâncias e excluindo os objetos do computador do cluster e seus respectivos nós do Active Directory.

Recursos adicionais

[Calculadora do Storage Spaces Direct \(Preview\)](#)

[Planejamento do Storage Spaces Direct](#)

[Visão geral do Storage Spaces Direct](#)

[Tolerância a falhas e eficiência de armazenamento no Storage Spaces Direct](#)

Recursos e tags

O Amazon EC2 fornece recursos diferentes que você pode criar e usar. Alguns desses recursos incluem imagens, instâncias, volumes e snapshots. Ao criar um recurso, atribuímos a ele um ID de recurso exclusivo.

Alguns recursos podem ser marcados com valores que você define, para ajudá-lo a organizá-los e identificá-los.

Os seguintes tópicos descrevem recursos e tags e como você pode trabalhar com eles.

Tópicos

- [Localizações de recursos \(p. 1544\)](#)
- [IDs de recursos \(p. 1545\)](#)
- [Listar e filtrar seus recursos \(p. 1546\)](#)
- [Marcar com tag os recursos do Amazon EC2 \(p. 1554\)](#)
- [Cotas de serviço do Amazon EC2 \(p. 1567\)](#)
- [Relatórios de uso do Amazon EC2 \(p. 1569\)](#)

Localizações de recursos

Os recursos do Amazon EC2 são específicos para a AWS Região ou zona de disponibilidade de residência.

Recurso	Tipo	Descrição
Identificadores de recursos do Amazon EC2	Regional	Cada identificador de recursos, como um ID de AMI, ID de instância, ID de volume do EBS ou ID de snapshot do EBS, é vinculado à sua região e só pode ser usado na região em que você criou o recurso.
Nomes de recursos fornecidos pelo usuário	Regional	Cada nome de recurso, como um nome de grupo de segurança ou de par de chaves, é vinculado à sua região e só pode ser usado na região em que você criou o recurso. Embora você possa criar recursos com o mesmo nome em várias regiões, eles não são relacionados uns aos outros.
AMIs	Regional	A AMI é vinculada à região onde seus arquivos estão localizados no Amazon S3. Você pode copiar uma AMI de uma região para outra. Para obter mais informações, consulte Copiar um AMI (p. 120) .
Snapshots do EBS	Regional	Um snapshot EBS é vinculado à sua região e só pode ser usado para criar volumes na mesma região. É possível copiar um snapshot de uma região em outra.

Recurso	Tipo	Descrição
		Para obter mais informações, consulte Copiar um snapshot do Amazon EBS. (p. 1317) .
Volumes do EBS	Availability Zone	Um volume do Amazon EBS é vinculado à sua zona de disponibilidade e só pode ser anexado a instâncias na mesma zona de disponibilidade.
Endereços IP elásticos	Regional	Um endereço IP elástico está vinculado a uma região e pode ser associado apenas a uma instância na mesma região.
Instâncias	Availability Zone	Uma instância é vinculada às zonas de disponibilidade na qual você a executou. Contudo, observe que o ID da instância está vinculado à região.
Pares de chaves	Global ou regional	Os pares de chaves criados com o Amazon EC2 são vinculados à região onde você os criou. Você pode criar seu próprio par de chaves de RSA e fazer upload dele na região em que deseja usá-lo; portanto, você pode tornar seu par de chaves globalmente disponível fazendo upload dele em cada região. Para obter mais informações, consulte Pares de chaves do Amazon EC2 e instâncias do Windows (p. 1209) .
Grupos de segurança	Regional	Um grupo de segurança é vinculado a uma região e pode ser atribuído somente a instâncias na mesma região. Você não pode permitir que uma instância se comunique com uma instância fora de sua região usando regras de grupo de segurança. O tráfego de uma instância em outra região é considerado como a largura de banda de WAN.

IDs de recursos

Ao criarmos recursos, atribuímos a cada um deles um ID de recurso exclusivo. Um ID de recurso assume a forma de um identificador de recurso (como `snap` para um snapshot), seguido de um hífen e uma combinação única de oito letras e números.

Cada identificador de recursos, como um ID de AMI, ID de instância, ID de volume do EBS ou ID de snapshot do EBS, é vinculado à sua região e só pode ser usado na região em que você criou o recurso.

Você pode usar IDs de recursos para localizar seus recursos no console do Amazon EC2. Se você estiver usando uma ferramenta de linha de comando ou a API do Amazon EC2 para trabalhar com o Amazon EC2, os IDs dos recursos serão necessários para determinados comandos. Por exemplo, se você estiver usando o comando `stop-instances` da AWS CLI para interromper uma instância, deverá especificar o ID da instância no comando.

Tamanho do ID do recurso

Antes de janeiro de 2016, os IDs atribuídos a recursos recém-criados de determinados tipos usavam 8 caracteres após o hífen (por exemplo, `i-1a2b3c4d`). De janeiro de 2016 a junho de 2018, alteramos os IDs desses tipos de recursos para 17 caracteres após o hífen (por exemplo, `i-1234567890abcdef0`). Dependendo de quando sua conta foi criada, é possível ter recursos dos tipos a seguir com IDs curtos, embora quaisquer novos recursos desses tipos recebam os IDs mais longos:

- bundle
- conversion-task
- customer-gateway
- dhcp-options
- elastic-ip-allocation
- elastic-ip-association
- export-task
- flow-log
- image
- import-task
- instância
- internet-gateway
- network-acl
- network-acl-association
- network-interface
- network-interface-attachment
- prefix-list
- route-table
- route-table-association
- security-group
- snapshot
- sub-rede
- subnet-cidr-block-association
- reserva
- volume
- vpc
- vpc-cidr-block-association
- vpc-endpoint
- vpc-peering-connection
- vpn-connection
- vpn-gateway

Listar e filtrar seus recursos

Você pode obter uma lista de alguns tipos de recursos usando o console do Amazon EC2. Você pode obter uma lista de cada tipo de recurso usando seu comando ou ação de API correspondente. Se você tiver muitos recursos, é possível filtrar os resultados para incluir ou excluir somente aqueles que correspondem a determinados critérios.

Tópicos

- [Listar e filtrar recursos usando o console \(p. 1547\)](#)
- [Listar e filtrar usando a CLI e a API \(p. 1551\)](#)

- [Listar e filtrar recursos entre Regiões usando o Amazon EC2 Global View \(p. 1553\)](#)

Listar e filtrar recursos usando o console

Sumário

- [Listar recursos usando o console \(p. 1547\)](#)
- [Filtrar recursos usando o console \(p. 1547\)](#)

Listar recursos usando o console

Você pode visualizar os tipos de recurso do Amazon EC2 mais comuns usando o console. Para ver os recursos adicionais, use a interface de linha de comando ou as ações de API.

Para listar os recursos do EC2 usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha a opção que corresponde ao tipo de recurso. Por exemplo, para listar suas instâncias, escolha Instances (Instâncias).

A página exibe todos os recursos do tipo de recurso selecionado.

Filtrar recursos usando o console

Para filtrar uma lista de recursos

1. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
2. Escolha o campo de pesquisa.
3. Escolha o filtro na lista.
4. Escolha um valor de filtro.
5. Quando terminar, remova o filtro.

A funcionalidade de pesquisa e filtro difere ligeiramente entre o console do Amazon EC2 antigo e o novo.

New console

O novo console oferece suporte a dois tipos de filtragem.

- A filtragem de API acontece no lado do servidor. A filtragem é aplicada na chamada de API, o que reduz o número de recursos retornados pelo servidor. Isso permite a filtragem rápida em grandes conjuntos de recursos e pode reduzir o tempo e o custo de transferência de dados entre o servidor e o navegador.
- A filtragem do cliente acontece no lado do cliente. Isso permite filtrar dados que já estão disponíveis no navegador (em outras palavras, dados que já foram retornados pela API). A filtragem do cliente funciona bem em conjunto com um filtro de API para filtrar para conjuntos de dados menores no navegador.

O novo console do Amazon EC2 é compatível com os seguintes tipos de pesquisa:

Pesquisa por palavra-chave

A pesquisa por palavra-chave é uma pesquisa de texto livre que permite pesquisar um valor em todos os atributos de seus recursos, sem especificar um atributo a ser pesquisado.

Note

Todas as pesquisas por palavras-chave usam filtragem do cliente.

Para pesquisar por palavra-chave, insira ou cole o que você procura na caixa de pesquisa e selecione Enter. Por exemplo, procurar 123 corresponde a todas as instâncias que têm 123 em qualquer um de seus atributos, como um endereço IP, ID de instância, ID de VPC ou ID de AMI. Se sua pesquisa de texto livre retornar correspondências inesperadas, aplique filtros adicionais.

Pesquisar por atributos

A pesquisa por um atributo permite que você pesquise um atributo específico em todos os recursos.

Note

As pesquisas de atributos usam filtragem de API ou filtragem de cliente, dependendo do atributo selecionado. Ao realizar uma pesquisa de atributo, os atributos são agrupados conforme necessário.

Por exemplo, é possível pesquisar o atributo Instance state (Estado da instância) para todas as instâncias para retornar apenas instâncias que estão no estado stopped. Para fazer isso:

1. No campo de pesquisa na tela Instances (Instâncias), comece inserindo `Instance state`. À medida que você insere os caracteres, os dois tipos de filtros aparecem para Instance state (Estado da instância): API filters (Filtros de API) e Client filters (Filtros de cliente).
2. Para pesquisar no lado do servidor, escolha Instance state (Estado da instância) em API filters (Filtros de API). Para pesquisar no lado do cliente, escolha Instance state (client) (Estado da instância (cliente)) em Client filters (Filtros de cliente).

Uma lista de valores possíveis para o atributo selecionado é exibida.

3. Selecione stopped (interrompido) na lista.

Você pode usar as seguintes técnicas para aprimorar ou refinar suas pesquisas:

Pesquisa inversa

Pesquisas inversas permitem pesquisar recursos que não correspondem a um valor especificado. Pesquisas inversas são realizadas colocando o caractere de ponto de exclamação (!) como prefixo da palavra-chave de pesquisa.

Note

A pesquisa inversa é compatível com pesquisas de palavras-chave e pesquisas de atributos somente em filtros de cliente. Ela não é compatível com pesquisas de atributos em filtros de API.

Por exemplo, é possível pesquisar o atributo Instance state (Estado da instância) para todas as instâncias a fim de excluir todas as instâncias que estão no estado terminated. Para fazer isso:

1. No campo de pesquisa na tela Instances (Instâncias), comece inserindo `Instance state`. À medida que você insere os caracteres, os dois tipos de filtros aparecem para Instance state (Estado da instância): API filters (Filtros de API) e Client filters (Filtros de cliente).
2. Escolha Instance state (client) (Estado da instância (cliente)). A pesquisa inversa é suportada somente em filtros de cliente.

Uma lista de valores possíveis para o atributo selecionado é exibida.

3. Insira ! (ponto de exclamação) para exibir os filtros inversos.

4. Escolha !terminated (!encerrado) na lista.

Para filtrar instâncias com base em um atributo de estado de instância, você também pode usar os ícones de pesquisa



) na coluna Instance state (Estado da instância). O ícone de pesquisa com um sinal de mais (+) exibe todas as instâncias que correspondem a esse atributo. O ícone de pesquisa com um sinal de menos (-) exclui todas as instâncias que correspondem a esse atributo.

Aqui está outro exemplo de uso da pesquisa inversa: listar todas as instâncias que não são atribuídas ao grupo de segurança chamado launch-wizard-1, pesquise pelo atributo Security group name (Nome do grupo de segurança) e, em palavra-chave, insira !launch-wizard-1.

Pesquisa parcial

Com pesquisas parciais, você pode procurar valores de string parciais. Para realizar uma pesquisa parcial, insira apenas uma parte da palavra-chave que você deseja pesquisar. Por exemplo, para pesquisar todas as instâncias t2.micro, t2.small e t2.medium, pesquise pelo atributo Instance Type (Tipo de instância) e, para a palavra-chave, insira t2.

Note

A pesquisa parcial é compatível com pesquisas de palavras-chave e pesquisas de atributos somente em filtros de cliente. Ela não é compatível com pesquisas de atributos em filtros de API.

Pesquisa de expressão regular

Para usar pesquisas de expressão regular, você deve habilitar Use regular expression matching (Usar correspondência de expressão regular) nas preferências.

As expressões regulares são úteis quando você precisa corresponder os valores de um campo com um padrão específico. Por exemplo, para procurar um valor que comece com s, procure ^s. Para procurar um valor que termine com xyz, procure xyz\$. Ou para procurar um valor que começa com um número seguido por um ou mais caracteres, procure [0-9]+.*. As pesquisas de expressão regular não diferenciam maiúsculas e minúsculas.

Note

A pesquisa de expressão regular é compatível com pesquisas de palavras-chave e pesquisas de atributos somente em filtros de cliente. Ela não é compatível com pesquisas de atributos em filtros de API.

Pesquisa por curinga

Use o curinga * para corresponder a zero ou mais caracteres. Use o curinga ? para corresponder a zero ou um caractere. Por exemplo, se você tiver um conjunto de dados com os seguintes valores: prod, prods e production; "prod*" corresponde a todos os valores, enquanto "prod?" corresponde apenas a prod e prods. Para usar os valores literais, coloque uma barra invertida (\) antes e depois deles. Por exemplo, "prod*" corresponderia a prod*.

Note

A pesquisa por curinga é compatível apenas com pesquisas de atributos em filtros de API. Não é compatível com pesquisas de palavras-chave e pesquisas de atributos somente em filtros de cliente.

Combinar pesquisas

Em geral, vários filtros com o mesmo atributo são unidos automaticamente com OR. Por exemplo, pesquisar Instance State : Running e Instance State : Stopped retorna todas as instâncias que estão em execução OU interrompidas. Para unir a pesquisa com AND, pesquise em

diferentes atributos. Por exemplo, procurar `Instance State : Running` e `Instance Type : c4.large` retorna apenas instâncias que são do tipo `c4.large` E que estão no estado parado.

Old console

O antigo console do Amazon EC2 é compatível com os seguintes tipos de pesquisa:

Pesquisa por palavra-chave

Pesquisa por palavra-chave é uma pesquisa de texto livre que permite que você procure um valor em todos os atributos de seus recursos. Para pesquisar por palavra-chave, insira ou cole o que você procura na caixa de pesquisa e selecione Enter. Por exemplo, procurar `123` corresponde a todas as instâncias que têm `123` em qualquer um de seus atributos, como um endereço IP, ID de instância, ID de VPC ou ID de AMI. Se sua pesquisa de texto livre retornar correspondências inesperadas, aplique filtros adicionais.

Pesquisar por atributos

A pesquisa por um atributo permite que você pesquise um atributo específico em todos os recursos. Por exemplo, você pode pesquisar o atributo Estado para todas as instâncias para retornar apenas instâncias que estão no estado `stopped`. Para fazer isso:

1. No campo de pesquisa na tela Instances (Instâncias), comece inserindo `Instance State`. À medida que você insere caracteres, uma lista de atributos correspondentes é exibida.
2. Selecione `Instance State` (Estado da instância) na lista. Uma lista de valores possíveis para o atributo selecionado é exibida.
3. Selecione `Stopped` (Parado) na lista.

Você pode usar as seguintes técnicas para aprimorar ou refinar suas pesquisas:

Pesquisa inversa

Pesquisas inversas permitem pesquisar recursos que não correspondem a um valor especificado. Pesquisas inversas são realizadas colocando o caractere de ponto de exclamação (!) como prefixo da palavra-chave de pesquisa. Por exemplo, para listar todas as instâncias que não foram encerradas, pesquise pelo atributo `InstanceState` (Estado da instância) e, para a palavra-chave, insira `!Terminated`.

Pesquisa parcial

Com pesquisas parciais, você pode procurar valores de string parciais. Para realizar uma pesquisa parcial, insira apenas uma parte da palavra-chave que deseja pesquisar. Por exemplo, para pesquisar todas as instâncias `t2.micro`, `t2.small` e `t2.medium`, pesquise pelo atributo `Instance Type` (Tipo de instância) e, para a palavra-chave, insira `t2`.

Pesquisa de expressão regular

As expressões regulares são úteis quando você precisa corresponder os valores de um campo com um padrão específico. Por exemplo, para pesquisar todas as instâncias que têm um valor de atributo que começa com `s`, procure `^s`. Ou para procurar todas as instâncias que têm um valor de atributo que termina com `xyz`, procure `xyz$`. As pesquisas de expressão regular não diferenciam maiúsculas e minúsculas.

Combinar pesquisas

Em geral, vários filtros com o mesmo atributo são unidos automaticamente com OR. Por exemplo, pesquisar `InstanceState : Running` e `InstanceState : Stopped` retorna todas as instâncias que estão em execução OU interrompidas. Para unir a pesquisa com AND, pesquise em diferentes atributos. Por exemplo, procurar `InstanceState : Running` e `Instance Type : c4.large` retorna apenas instâncias que são do tipo `c4.large` E que estão no estado parado.

Listar e filtrar usando a CLI e a API

Cada tipo de recurso tem um comando da CLI correspondente e ação de API que você usa para listar os recursos desse tipo. As listas de recursos resultantes podem ser longas, portanto, pode ser mais rápido e mais útil filtrar os resultados para incluir apenas os recursos que correspondem a critérios específicos.

Considerações sobre filtragem

- Você pode especificar vários filtros e vários valores de filtro em uma única solicitação.
- Você também pode usar caracteres curinga com os valores de filtro. Um asterisco (*) corresponde a zero ou mais caracteres, e um ponto de interrogação (?) corresponde a zero ou um caractere.
- Os valores do filtro diferenciam maiúsculas de minúsculas.
- Sua pesquisa pode incluir os valores literais dos caracteres curinga; apenas só precisa recuá-los uma barra invertida antes do caractere. Por exemplo, um valor *amazon\?\?\ pesquisaria pela string literal, *amazon?.

Filtros compatíveis

Para ver os filtros compatíveis com cada recurso do Amazon EC2, consulte a documentação a seguir:

- AWS CLI: os comandos `describe` na [AWS CLI Command Reference-Amazon EC2](#) (Referência de comandos da AWS CLI - Amazon EC2).
- Tools for Windows PowerShell: os comandos `Get` na [AWS Tools for PowerShell Cmdlet Reference-Amazon EC2](#) (Referência de cmdlets do AWS Tools for Windows PowerShell - Amazon EC2).
- API de consulta: as ações `Describe` da API na [Amazon EC2 API Reference](#) (Referência da API do Amazon EC2).

Example Exemplo: Especificar um único filtro

Você pode listar suas instâncias do Amazon EC2 usando `describe-instances`. Sem filtros, a resposta contém informações de todos os recursos. Você pode usar o seguinte comando para incluir apenas as instâncias em execução em sua saída.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running
```

Para listar apenas os IDs de suas instâncias em execução, adicione o parâmetro `--query` da seguinte maneira.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running --query "Reservations[*].Instances[*].InstanceId" --output text
```

A seguir está um exemplo de saída.

```
i-0ef1f57f78d4775a4
i-0626d4edd54f1286d
i-04a636d18e83cfacb
```

Example Exemplo: Especificar vários filtros ou valores de filtro

Se você especificar vários filtros ou vários valores de filtro, o recurso deverá corresponder a todos os filtros a serem incluídos nos resultados.

Você pode usar o seguinte comando para listar todas as instâncias cujo tipo é `m5.large` ou `m5d.large`.

```
aws ec2 describe-instances --filters Name=instance-type,Values=m5.large,m5d.large
```

Você pode usar o seguinte comando para listar todas as instâncias paradas cujo tipo é `t2.micro`.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=stopped Name=instance-type,Values=t2.micro
```

Example Exemplo: Usar curingas em um valor de filtro

Se você especificar `database` como o valor do filtro `description` ao descrever snapshots do EBS usando [describe-snapshots](#), o comando retornará somente os snapshots cuja descrição é “banco de dados”.

```
aws ec2 describe-snapshots --filters Name=description,Values=database
```

O curinga `*` corresponde a zero ou mais caracteres. Se você especificar `*database*` como o valor do filtro, o comando retornará apenas snapshots cuja descrição inclui a palavra banco de dados.

```
aws ec2 describe-snapshots --filters Name=description,Values=*database*
```

O curinga `?` corresponde exatamente a 1 caractere. Se você especificar `database?` como o valor do filtro, o comando retornará apenas snapshots cuja descrição é “banco de dados” ou “banco de dados” seguido por um caractere.

```
aws ec2 describe-snapshots --filters Name=description,Values=database?
```

Se você especificar `database????`, o comando retornará apenas snapshots cuja descrição é “banco de dados” seguida de até quatro caracteres. Ele exclui descrições com “banco de dados” seguido por cinco ou mais caracteres.

```
aws ec2 describe-snapshots --filters Name=description,Values=database????
```

Example Exemplo: filtro baseado em data

Com a AWS CLI, você pode usar JMESPath para filtrar resultados usando expressões. Por exemplo, o comando [describe-snapshots](#) a seguir exibe os IDs de todos os snapshots criados pela sua conta da AWS(representada por `123456789012`) antes da data especificada (representada por `31/3/2020`). Se você não especificar o proprietário, os resultados incluirão todos os snapshots públicos.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

O comando a seguir exibe os IDs de todos os snapshots criados no intervalo de datas especificado.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]" --output text
```

Filtrar com base em tags

Para obter exemplos de como filtrar uma lista de recursos de acordo com suas tags, consulte [Trabalhar com tags usando a linha de comando \(p. 1563\)](#).

Listar e filtrar recursos entre Regiões usando o Amazon EC2 Global View

O Amazon EC2 Global View permite que você visualize alguns de seus recursos do Amazon EC2 e do Amazon VPC em uma única Região AWS ou em várias Regiões em um único console. Usando o Amazon EC2 Global View, você pode visualizar um resumo de todas as suas VPCs, sub-redes, instâncias, grupos de segurança e volumes em todas as Regiões para as quais sua conta AWS está habilitada. O Amazon EC2 Global View também fornece a funcionalidade pesquisa global, que permite pesquisar recursos específicos ou tipos de recursos específicos em várias Regiões simultaneamente.

O Amazon EC2 Global View não permite que você modifique recursos de forma alguma.

Permissões obrigatórias

Um usuário do IAM deve ter as seguintes permissões para usar o Amazon EC2 Global View.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeInstances",  
                "ec2:DescribeVpcs",  
                "ec2:DescribeRegions",  
                "ec2:DescribeVolumes",  
                "ec2:DescribeSubnets",  
                "ec2:DescribeSecurityGroups"  
            ],  
            "Resource": "*"  
        }]  
    }  
}
```

Para usar o Amazon EC2 Global View

Abra o console do Amazon EC2 Global View em <https://console.aws.amazon.com/ec2globalview/home>.

O console consiste em duas abas:

- Explorador de Região: essa aba inclui as seções a seguir:
 - Resumo do recurso: fornece uma visão geral de alto nível dos recursos em todas as Regiões.

Regiões habilitadas indica o número de Regiões para as quais sua conta AWS está habilitada. Os campos restantes indicam o número de recursos que você tem atualmente nessas Regiões. Escolha qualquer um dos links para exibir os recursos desse tipo em todas as Regiões. Por exemplo, se o link abaixo do rótulo Instâncias for 29 em 10 Regiões, ele indica que você tem 29 instâncias em 10 Regiões. Escolha o link para visualizar uma lista de todas as 29 instâncias.

- Contagens de recursos por Região: lista todas as Regiões AWS (incluindo aquelas para as quais sua conta não está habilitada) e fornece o número total para cada tipo de recurso para cada Região.

Escolha um nome de Região para exibir todos os recursos de todos os tipos para essa Região específica. Por exemplo, escolha África (Cidade do Cabo) af-south-1 para visualizar todas as VPCs, sub-redes, instâncias, grupos de segurança e volumes nessa Região. Como alternativa, selecione uma Região e escolha Exibir recursos para a Região selecionada.

Escolha o valor para um tipo de recurso específico em uma Região específica para exibir somente os recursos desse tipo nessa Região. Por exemplo, escolha o valor para Instâncias para África (Cidade do Cabo) af-south-1 para exibir somente as instâncias nessa Região.

- Pesquisa global: essa guia permite que você pesquise recursos específicos ou tipos de recursos específicos em uma única Região ou em várias Regiões. Ela também permite que você veja detalhes de um recurso específico.

Para pesquisar recursos, insira os critérios de pesquisa no campo anterior à grade. Você pode pesquisar por Região, por tipo de recurso e pelas etiquetas atribuídas aos recursos.

Para visualizar os detalhes de um recurso específico, selecione-o na grade. Você também pode escolher o ID de recurso para abrir o recurso no respectivo console. Por exemplo, escolha um ID de instância para abrir a instância no console do Amazon EC2 ou escolha um ID de sub-rede para abrir a sub-rede no console da Amazon VPC.

Marcar com tag os recursos do Amazon EC2

Para ajudá-lo a gerenciar instâncias, imagens e outros recursos do Amazon EC2, é possível atribuir seus próprios metadados a cada recurso na forma de tags. As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Isso é útil quando você tem muitos recursos do mesmo tipo — é possível identificar rapidamente um recurso específico baseado nas tags que você atribuiu a ele. Este tópico descreve tags e mostra a você como criá-los.

Warning

As chaves de tag e seus valores são apresentados por várias chamadas de API diferentes. Negar acesso ao `DescribeTags` não nega automaticamente acesso às tags apresentadas por outras APIs. Como uma prática recomendada, sugerimos que você não inclua dados confidenciais nas suas tags.

Tópicos

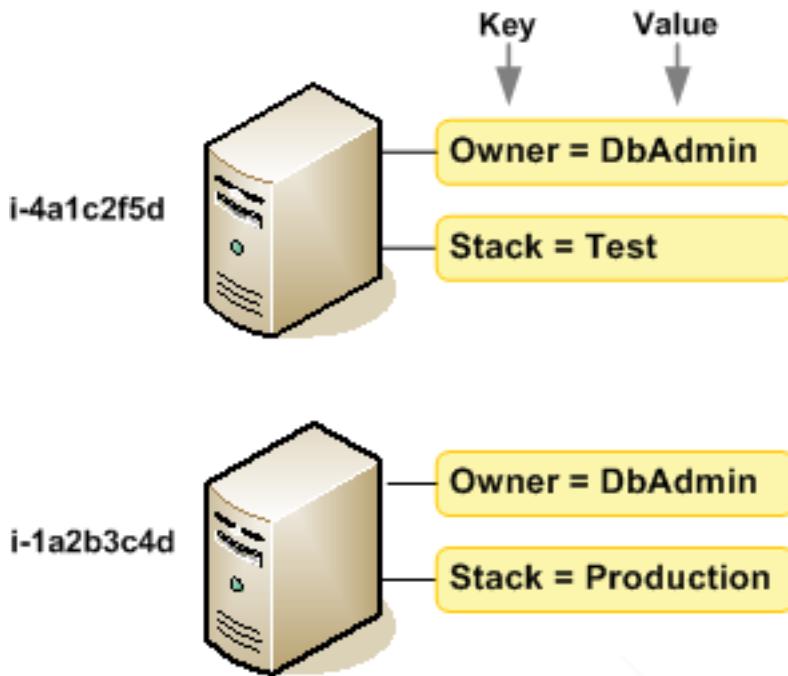
- [Conceitos básicos de tags \(p. 1554\)](#)
- [Marcar com tag os recursos do \(p. 1555\)](#)
- [Restrições de tags \(p. 1558\)](#)
- [Gerenciamento de tags e acesso \(p. 1559\)](#)
- [Marcar com tag recursos para faturamento \(p. 1559\)](#)
- [Trabalhar com tags usando o console \(p. 1560\)](#)
- [Trabalhar com tags usando a linha de comando \(p. 1563\)](#)
- [Adicionar tags a um recurso usando o CloudFormation \(p. 1566\)](#)

Conceitos básicos de tags

Uma tag é um rótulo atribuído a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional, ambos definidos por você.

As tags permitem categorizar seus recursos da AWS de diferentes formas (como por finalidade, por proprietário ou por ambiente). Por exemplo, você pode definir um conjunto de tags para as instâncias do Amazon EC2 da sua conta que lhe ajudem a rastrear o proprietário e o nível do stack de cada instância.

O diagrama a seguir mostra como funciona o uso de tags. Neste exemplo, você atribuiu duas tags a cada uma de suas instâncias — uma tag com a chave `Owner` e outra com a chave `Stack`. Cada tag tem também um valor associado.



Recomendamos que você desenvolva um conjunto de chave de tags que atenda suas necessidades para cada tipo de recurso. Usar um conjunto consistente de chaves de tags facilita para você gerenciar seus recursos. Você pode pesquisar e filtrar os recursos de acordo com as tags que adicionar. Para obter mais informações sobre como implementar uma estratégia eficaz de marcação de recursos, consulte o whitepaper da AWS, [Tagging Best Practices](#) (Práticas recomendadas de marcação).

As tags não têm significado semântico no Amazon EC2 e são interpretadas estritamente como uma sequência dos caracteres. Além disso, as tags não são automaticamente atribuídas aos seus recursos. Você pode editar chaves de tags e valores, e você pode remover as tags de um recurso a qualquer momento. Você pode definir o valor de uma tag a uma string vazia, mas não pode configurar o valor de um tag como nula. Se você adicionar uma tag que tenha a mesma chave de uma tag existente nesse recurso, o novo valor substituirá o antigo. Se você excluir um recurso, todas as tags do recurso também serão excluídas.

Note

Depois de excluir um recurso, suas etiquetas podem permanecer visíveis nas saídas do console, API e CLI por um curto período. Essas etiquetas serão gradualmente desassociadas do recurso e serão excluídas permanentemente.

Marcar com tag os recursos do

Você pode usar tags na maioria dos recursos do Amazon EC2 que já existem na sua conta. A [tabela \(p. 1556\)](#) a seguir lista os recursos compatíveis com o uso de tags.

Se você estiver usando o console do Amazon EC2, poderá aplicar tags aos recursos usando a guia Tags na tela de recursos relevante ou usar a tela Tags. Algumas telas de recursos permitem que você especifique tags para um recurso ao criá-lo; por exemplo, uma tag com uma chave de Name e um valor que você especificar. Na maioria dos casos, o console aplicará as tags imediatamente depois de o recurso

ser criado (em vez de durante a criação de recursos). O console pode organizar os recursos de acordo com a tag do Name, mas ela não tem nenhum significado semântico ao serviço do Amazon EC2.

Se você estiver usando a API do Amazon EC2, a AWS CLI ou o AWS SDK, poderá usar a ação `CreateTags` da API do EC2 para aplicar tags aos recursos existentes. Além disso, algumas ações de criação de recursos permitem que você especifique tags para um recurso quando ele é criado. Se as tags não puderem ser aplicadas durante a criação dos recursos, nós reverteremos o processo de criação de recursos. Isso garante que os recursos sejam criados com tags ou, então, não criados, e que nenhum recurso seja deixado sem tags. Ao marcar com tags os recursos no momento da criação, você elimina a necessidade de executar scripts personalizados de uso de tags após a criação do recurso. Para obter mais informações sobre como permitir que os usuários marquem os recursos durante a criação, consulte [Conceder permissão para marcar recursos durante a criação \(p. 1145\)](#).

A tabela a seguir descreve os recursos do Amazon EC2 que podem ser marcados e os recursos que podem ser marcados na criação usando a API do Amazon EC2, a AWS CLI ou um AWS SDK.

Suporte à marcação para recursos do Amazon EC2

Recurso	Compatível com tags	Oferece suporte à marcação na criação
AFI	Sim	Sim
AMI	Sim	Sim
Tarefa de pacote	Não	Não
Capacity Reservation	Sim	Sim
Gateway da operadora	Sim	Sim
Endpoint do Client VPN	Sim	Sim
Rota do Client VPN	Não	Não
Gateway do cliente	Sim	Sim
Dedicated Host	Sim	Sim
Reserva de Host dedicado	Sim	Sim
Opção de DHCP	Sim	Sim
Snapshot do EBS	Sim	Sim
Volume do EBS	Sim	Sim
EC2 Fleet	Sim	Sim
Gateway da Internet somente de saída	Sim	Sim
Endereços elastic IP (EIPs)	Sim	Sim
Aceleradora do Elastic Graphics	Sim	Não
Instância	Sim	Sim
Volumes de armazenamento de instâncias	N/D	N/D
Gateway da Internet	Sim	Sim

Recurso	Compatível com tags	Oferece suporte à marcação na criação
Grupo de endereços IP (BYOIP)	Sim	Sim
Par de chaves	Sim	Sim
Modelo de execução	Sim	Sim
Versão do modelo de execução	Não	Não
Gateway local	Sim	Não
Tabela de rotas do gateway local	Sim	Não
Interface virtual do gateway local	Sim	Não
Grupo de interface virtual do gateway local	Sim	Não
Associação de VPC da tabela de rotas do gateway local	Sim	Sim
Associação de grupos de interface virtual da tabela de rotas do gateway local	Sim	Não
gateway NAT	Sim	Sim
Conexão ACL	Sim	Sim
Interface de rede	Sim	Sim
Placement group	Sim	Sim
Lista de prefixos	Sim	Sim
Reserved Instance	Sim	Não
Listagem do Instância reservada	Não	Não
Tabela de rotas	Sim	Sim
Solicitação de frota spot	Sim	Sim
Solicitação de instância Spot	Sim	Sim
Grupo de segurança	Sim	Sim
Regra do grupo de segurança	Sim	Não
Sub-rede	Sim	Sim
Filtro de espelho de tráfego	Sim	Sim
Sessão de espelho de tráfego	Sim	Sim
Destino de espelho de tráfego	Sim	Sim
Transit gateway	Sim	Sim
Tabela de rotas do Transit Gateway	Sim	Sim

Recurso	Compatível com tags	Oferece suporte à marcação na criação
Anexo da VPC do Transit Gateway	Sim	Sim
Gateway privado virtual	Sim	Sim
VPC	Sim	Sim
VPC endpoint	Sim	Sim
Serviço de VPC endpoint	Sim	Sim
Configuração do serviço do VPC endpoint	Sim	Sim
Log do fluxo da VPC	Sim	Sim
Conexão de emparelhamento de VPC	Sim	Sim
Conexão VPN	Sim	Sim

Você pode marcar instâncias e volumes durante a criação usando o assistente de instâncias do Amazon EC2 Launch no console do Amazon EC2. Você pode marcar com tag seus volumes do EBS na criação usando a tela Volumes ou snapshots do EBS usando a tela Snapshots. Se preferir, use as APIs do Amazon EC2 para criação de recursos (por exemplo, [RunInstances](#)) para aplicar tags ao criar seu recurso.

Você pode aplicar permissões no nível do recurso com base em tags nas suas políticas do IAM para ações de API do Amazon EC2 que oferecem suporte à marcação durante a criação para implementar controle granular sobre os usuários e grupos que podem marcar recursos na criação. Seus recursos estão devidamente protegidos contra criação — as tags aplicadas imediatamente aos recursos; portanto, todas as permissões em nível de recurso baseadas em tags que controlam o uso de recursos entram imediatamente em vigor. Seus recursos podem ser rastreados e relatados com mais precisão. Você pode obrigar o uso de marcação com tags nos novos recursos e controlar quais chaves e valores de tag são definidos nos seus recursos.

Você também pode aplicar permissões em nível de recurso às ações `CreateTags` e `DeleteTags` da API do Amazon EC2 nas suas políticas do IAM, de forma a controlar quais chaves e valores de tags são definidos nos recursos existentes. Para obter mais informações, consulte [Exemplo: marcar recursos \(p. 1178\)](#).

Para obter mais informações sobre como marcar os seus recursos para o faturamento, consulte [Using cost allocation tags](#) (Usar tags de alocação de custos) no AWS Billing and Cost Management User Guide (Manual do usuário do AWS Billing and Cost Management).

Restrições de tags

As restrições básicas a seguir se aplicam às tags:

- Número máximo de tags por recurso – 50
- Em todos os recursos, cada chave de tag deve ser exclusiva e pode ter apenas um valor.
- Comprimento máximo da chave – 128 caracteres Unicode em UTF-8
- Comprimento máximo do valor – 256 caracteres Unicode em UTF-8

- Embora o EC2 permita qualquer caractere em suas tags, outros serviços podem ser mais restritivos. Os caracteres permitidos nos serviços são: letras, números e espaços representáveis em UTF-8 e os seguintes caracteres: + - = . _ : / @.
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- O prefixo aws : é reservado para uso da AWS. Não é possível editar nem excluir a chave ou o valor de uma tag quando ela tem uma chave de tag com esse prefixo. As tags com o prefixo aws : não contam para as tags por limite de recurso.

Você não pode encerrar, parar ou excluir um recurso baseado unicamente em suas tags; será preciso especificar o identificador de recursos. Por exemplo, para excluir snapshots marcados com uma chave de tag chamada DeleteMe, você deve usar a ação `DeleteSnapshots` com os identificadores de recursos dos snapshots, como `snap-1234567890abcdef0`.

Quando você marca recursos públicos ou compartilhados, as tags atribuídas ficam disponíveis somente para sua conta da AWS. Nenhuma outra conta da AWS terá acesso a essas tags. Para controle de acesso baseado em tags a recursos compartilhados, cada conta da AWS deve atribuir seu próprio conjunto de tags para controlar o acesso ao recurso.

Você não pode marcar com tag todos os recursos. Para obter mais informações, consulte [Suporte à marcação para recursos do Amazon EC2 \(p. 1556\)](#).

Gerenciamento de tags e acesso

Se você estiver usando o AWS Identity and Access Management (IAM), pode controlar quais usuários na sua conta da AWS têm permissão para criar, editar ou excluir tags. Para obter mais informações, consulte [Conceder permissão para marcar recursos durante a criação \(p. 1145\)](#).

Você também pode usar tags de recurso para implementar o controle baseado em atributo (ABAC). Você pode criar políticas do IAM que permitem operações com base nas tags do recurso. Para obter mais informações, consulte [Controlar o acesso aos recursos do EC2 usando tags de recursos \(p. 1147\)](#).

Marcar com tag recursos para faturamento

Também é possível usar tags para organizar sua conta da AWS para refletir sua própria estrutura de custo. Para isso, inscreva-se para obter sua conta da AWS com os valores de chave de tag incluídos. Para obter mais informações sobre como configurar um relatório de alocação de custos com tags, consulte [Relatório mensal de alocação de custos](#) no Manual do usuário do AWS Billing and Cost Management. Para ver o custo dos recursos combinados, você pode organizar as informações de faturamento com base nos recursos com os mesmos valores da chave da tag. Por exemplo, você pode etiquetar vários recursos com um nome de aplicação específico, e depois organizar suas informações de faturamento para ver o custo total daquela aplicação em vários serviços. Para obter mais informações, consulte [Using cost allocation tags](#)(Usar tags de alocação de custos) no AWS Billing and Cost Management User Guide (Manual do usuário do AWS Billing and Cost Management).

Note

Se você tiver acabado de habilitar a criação de relatórios, os dados do mês atual estarão disponíveis para visualização após 24 horas.

Tags de alocação de custos podem indicar quais recursos estão contribuindo para os custos, mas excluí-los ou desativá-los nem sempre reduz custos. Por exemplo, os dados de snapshots consultados por outro snapshot são preservados, mesmo se o snapshot que contém os dados originais for excluído. Para obter mais informações, consulte [Amazon Elastic Block Store volumes and snapshots](#) (Volumes e snapshots do Amazon Elastic Block Store) no AWS Billing and Cost Management User Guide (Manual do usuário do AWS Billing and Cost Management).

Note

Os endereços IP elásticos marcados não são exibidos no seu relatório de alocação de custos.

Trabalhar com tags usando o console

Usando o console do Amazon EC2, você pode ver quais tags estão em uso em todos os recursos do Amazon EC2 na mesma Região. Você pode visualizar tags por recurso e por tipo de recurso, e também verificar quantos itens de cada tipo de recurso está associado a uma tag especificada. Você também pode usar o console do Amazon EC2 para aplicar ou remover tags de um ou mais recursos por vez.

Para obter mais informações sobre o uso de filtros ao listar seus recursos, consulte [Listar e filtrar seus recursos \(p. 1546\)](#).

Para facilidade de uso e melhores resultados, use o Tag Editor no AWS Management Console, que fornece uma forma unificada e central para criar e gerenciar suas tags. Para obter mais informações, consulte [Tag Editor \(Editor de tags\)](#) em Getting Started with the AWS Management Console. (Conceitos básicos do AWS Management Console).

Tarefas

- [Exibir tags \(p. 1560\)](#)
- [Adicionar e excluir tags em um recurso individual \(p. 1561\)](#)
- [Adicionar e excluir tags a um grupo de recursos \(p. 1562\)](#)
- [Adicionar uma tag ao executar uma instância \(p. 1562\)](#)
- [Filtrar uma lista de recursos por tag \(p. 1563\)](#)

Exibir tags

Você pode exibir tags de duas maneiras diferentes no console do Amazon EC2. É possível exibir as tags para um recurso individual ou para todos os recursos.

Exibir tags para recursos individuais

Quando você selecionar uma página específica do recurso no console do Amazon EC2, ela exibirá uma lista desses recursos. Por exemplo, se você selecionar Instances (Instâncias) no painel de navegação, o console exibirá uma lista das instâncias do Amazon EC2. Ao selecionar um recurso de uma dessas listas (por exemplo, uma instância), se o recurso é compatível com tags, você pode ver e gerenciá-las. Na maioria das páginas de recursos, é possível visualizar as tags ao escolher a guia Tags.

Você pode adicionar uma coluna à lista de recursos que mostra todos os valores das tags com a mesma chave. Você pode usar essa coluna para classificar e filtrar a lista de recursos pela tag.

New console

- Escolha o ícone Preferences (Preferências) com a engrenagem no canto superior direito da tela. Na caixa de diálogo Preferences (Preferências), em Tag columns (Etiquetar colunas), selecione uma ou mais chaves de tag e escolha Confirm (Confirmar).

Old console

Há duas maneiras de adicionar uma coluna nova à lista de recursos para exibir suas tags:

- Na guia Tags, selecione Mostrar coluna. Uma nova coluna será adicionada ao console.
- Escolha o ícone de engrenagem Mostrar/ocultar colunas e a caixa de diálogo Mostrar/ocultar colunas, selecione a chave de tags em Suas chaves de tag.

Exibir tags para todos os recursos

Você pode exibir as tags em todos os recursos selecionando Tags no painel de navegação do console do Amazon EC2. A imagem a seguir mostra o painel Tags, que lista todas as tags em uso por tipo de recurso.

The screenshot shows a table titled "Manage Tags" with the following data:

	Tag Key	Tag Value	Total	Instances	AMIs	Volumes
Manage Tag	Name	DNS Server	1	1	0	0
Manage Tag	Owner	TeamB	2	0	0	2
Manage Tag	Owner	TeamA	2	0	0	2
Manage Tag	Purpose	Project2	1	0	0	1
Manage Tag	Purpose	Logs	1	0	0	1
Manage Tag	Purpose	Network Management	1	1	0	0
Manage Tag	Purpose	Project1	2	0	0	2

Adicionar e excluir tags em um recurso individual

Você pode gerenciar as tags para um recurso individual diretamente pela página de recursos.

Para adicionar uma tag a um recurso individual

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a Região que atende às suas necessidades. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre Regiões, enquanto outros não podem. Para obter mais informações, consulte [Localizações de recursos \(p. 1544\)](#).
3. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
4. Selecione o recurso da lista de recursos e escolha a guia Tags.
5. Escolha Manage tags (Gerenciar tags), Add tag (Adicionar tag). Insira a chave e o valor da tag. Quando terminar de adicionar tags, selecione Save (Salvar).

Para excluir uma tag de um recurso individual

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a Região que atende às suas necessidades. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre Regiões, enquanto outros não podem. Para obter mais informações, consulte [Localizações de recursos \(p. 1544\)](#).
3. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
4. Selecione o recurso da lista de recursos e escolha a guia Tags.
5. Selecione Manage tags (Gerenciar tags). Em cada tag, escolha Remove (Remover). Ao finalizar a remoção de tags, escolha Save (Salvar).

Adicionar e excluir tags a um grupo de recursos

Para adicionar uma tag a um grupo de recursos

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a Região que atende às suas necessidades. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre Regiões, enquanto outros não podem. Para obter mais informações, consulte [Localizações de recursos \(p. 1544\)](#).
3. No painel de navegação, selecione Tags.
4. Na parte superior do painel de conteúdo, escolha Gerenciar tags.
5. Em Filter (Filtro), selecione o tipo de recurso (por exemplo, instâncias).
6. Na lista de recursos, marque a caixa de seleção ao lado de cada recurso.
7. Em Add Tag (Adicionar tag), insira a chave e o valor da tag e escolha Add Tag (Adicionar tag).

Note

Se você adicionar uma nova tag com a mesma chave de uma tag existente, a nova sobrescreverá a tag existente.

Para remover uma tag de um grupo de recursos

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione a Região que atende às suas necessidades. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre Regiões, enquanto outros não podem. Para obter mais informações, consulte [Localizações de recursos \(p. 1544\)](#).
3. No painel de navegação, selecione Tags, Gerenciar tags.
4. Para ver as tags em uso, selecione o ícone de engrenagem Mostrar/ocultar colunas e, na caixa de diálogo Mostrar/ocultar colunas, selecione as chaves das tags e selecione Fechar.
5. Em Filter (Filtro), selecione o tipo de recurso (por exemplo, instâncias).
6. Na lista de recursos, marque a caixa de seleção ao lado de cada recurso.
7. Em Remove Tag (Remover tag), insira a chave da tag e escolha Remove Tag (Remover tag).

Adicionar uma tag ao executar uma instância

Para adicionar uma tag usando o Launch Wizard

1. Na barra de navegação, selecione a Região da instância. Essa escolha é importante, pois alguns recursos do Amazon EC2 podem ser compartilhados entre Regiões, enquanto outros não podem. Selecione a Região que satisfaça suas necessidades. Para obter mais informações, consulte [Localizações de recursos \(p. 1544\)](#).
2. Escolha Launch Instance (Executar instância).
3. A página Choose an Amazon Machine Image (AMI) (Escolher uma Imagem de máquina da Amazon (AMI)) exibe uma lista de configurações básicas denominadas Imagens de máquina da Amazon (AMI). Selecione as AMIs a serem usadas e escolha Selecionar. Para obter mais informações, consulte [Localizar uma AMI do Windows \(p. 102\)](#).
4. Na página Configurar detalhes da instância, configure as configurações da instância conforme necessário e selecione Próximo: Adicionar armazenamento.
5. Na página Adicionar armazenamento, especifique os volumes de armazenamento adicionais para sua instância. Selecione Próximo: Adicionar tags ao concluir.

6. Na página Adicionar tags, especifique tags da instância, os volumes ou ambos. Escolha Adicionar outra tag para adicionar mais de uma tag à sua instância. Escolha Next: Configure Security Group ao concluir.
7. Na página Configurar security group, escolha qualquer security group existente que você possui ou deixe o assistente criar um novo security group para você. Selecione Revisar e executar ao concluir.
8. Examine suas configurações. Quando você estiver satisfeito com suas seleções, escolha Executar. Selecione um par de chaves existente ou crie um novo, selecionando a caixa de confirmação e escolhendo Executar instâncias.

Filtrar uma lista de recursos por tag

Você pode filtrar sua lista de recursos baseados em uma ou mais chaves e valores de tags.

Para filtrar uma lista de recursos por tag

1. No painel de navegação, selecione um tipo de recurso (por exemplo, Instâncias).
2. Escolha o campo de pesquisa.
3. Escolha a chave de tag na lista.
4. Escolha o valor de tag correspondente na lista.
5. Quando terminar, remova o filtro.

Para obter mais informações sobre os filtros, consulte [Listar e filtrar seus recursos \(p. 1546\)](#).

Trabalhar com tags usando a linha de comando

É possível adicionar tags a muitos recursos do EC2 ao criá-las, usando o parâmetro de especificações de tag para o comando de criação. É possível visualizar as tags de um recurso usando o comando de descrição para o recurso. Também é possível adicionar, atualizar ou excluir tags para seus recursos existentes usando os seguintes comandos.

Tarefa	AWS CLI	AWS Tools for Windows PowerShell
Adicione ou substitua uma ou mais tags	create-tags	New-EC2Tag
Exclua uma ou mais tags	delete-tags	Remove-EC2Tag
Descreva uma ou mais tags	describe-tags	Get-EC2Tag

Tarefas

- [Adicionar tags na criação de recursos \(p. 1563\)](#)
- [Adicionar tags a um recurso existente \(p. 1564\)](#)
- [Descrever recursos marcados com tags \(p. 1565\)](#)

Adicionar tags na criação de recursos

Os exemplos a seguir demonstram como aplicar tags ao criar recursos.

A maneira como insere os parâmetros formatados pelo JSON na linha de comando difere dependendo de seu sistema operacional. Linux, macOS ou Unix e Windows PowerShell usam as aspas simples ('')

para delimitar a estrutura de dados JSON. Omita as únicas citações ao usar os comandos com a linha de comando do Windows. Para obter mais informações, consulte [Specifying parameter values for the AWS CLI](#) (Especificar valores de parâmetro para a CLI).

Example Exemplo: execute uma instância e aplique tags à instância e ao volume

O seguinte comando [run-instances](#) inicia uma instância e aplica uma tag com a chave **webserver** e o valor **production** à instância. O comando também aplica uma tag com uma chave de **cost-center** e um valor de **cc123** a qualquer volume do EBS criado (neste caso, o volume do dispositivo raiz).

```
aws ec2 run-instances \
--image-id ami-abc12345 \
--count 1 \
--instance-type t2.micro \
--key-name MyKeyPair \
--subnet-id subnet-6e7f829e \
--tag-specifications 'ResourceType=instance,Tags=[{Key=webserver,Value=production}]' \
'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Você pode aplicar as mesmas chaves da tag e os mesmos valores aos dois volumes e instâncias durante a execução. O comando a seguir executa uma instância e aplica uma tag com uma chave de **cost-center** e um valor de **cc123** à instância e a qualquer volume do EBS criado.

```
aws ec2 run-instances \
--image-id ami-abc12345 \
--count 1 \
--instance-type t2.micro \
--key-name MyKeyPair \
--subnet-id subnet-6e7f829e \
--tag-specifications 'ResourceType=instance,Tags=[{Key=cost-center,Value=cc123}]' \
'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Example Exemplo: crie um o volume e aplique uma tag

O comando [create-volume](#) cria um volume e aplica duas tags: **purpose=production** e **cost-center=cc123**.

```
aws ec2 create-volume \
--availability-zone us-east-1a \
--volume-type gp2 \
--size 80 \
--tag-specifications 'ResourceType=volume,Tags=[{Key=purpose,Value=production}, \
{Key=cost-center,Value=cc123}]'
```

Adicionar tags a um recurso existente

Os exemplos a seguir demonstram como adicionar tags a um recurso existente usando o comando [create-tags](#).

Example Exemplo: adicionar uma tag a um recurso

O seguinte comando adiciona a tag **Stack=production** à imagem especificada ou substitui uma tag existente para a AMI na qual a chave de tag é **Stack**. Se o comando for bem-sucedido, nenhuma saída será retornada.

```
aws ec2 create-tags \
--resources ami-78a54011 \
```

```
--tags Key=Stack,Value=production
```

Example Exemplo: adicionar tags a vários recursos

Este exemplo adiciona (ou substitui) duas tags para uma AMI e uma instância. Uma das tags contém apenas uma chave (**webserver**), sem valor (definimos o valor como uma string vazia). A outra tag consiste em uma chave (**stack**) e um valor (**Production**). Se o comando for bem-sucedido, nenhuma saída será retornada.

```
aws ec2 create-tags \  
  --resources ami-1a2b3c4d i-1234567890abcdef0 \  
  --tags Key=webserver,Value= Key=stack,Value=Production
```

Example Exemplo: adicionar tags com caracteres especiais

Este exemplo adiciona a tag [**Group**]=**test** a uma instância. Os colchetes ([e]) são caracteres especiais, que devem ser recuados.

Se você estiver usando o Linux ou o OS X, para recuar os caracteres especiais, coloque o elemento com o caractere especial entre aspas duplas ("") e coloque toda a estrutura de chave e valor entre aspas simples ('').

```
aws ec2 create-tags \  
  --resources i-1234567890abcdef0 \  
  --tags 'Key="[Group]",Value=test'
```

Se você estiver usando o Windows, para recuar os caracteres especiais, coloque o elemento que tem caracteres especiais entre aspas duplas ("") e preceda cada caractere de aspas duplas com uma barra invertida (\) da seguinte maneira:

```
aws ec2 create-tags ^  
  --resources i-1234567890abcdef0 ^  
  --tags Key=\"[Group]\",Value=test
```

Se você estiver usando o Windows PowerShell, para recuar os caracteres especiais, coloque o valor que tem caracteres especiais entre aspas duplas (""), preceda cada caractere de aspas duplas com uma barra invertida (\) e coloque toda a estrutura de chave e valor entre aspas simples ('') da seguinte maneira:

```
aws ec2 create-tags `  
  --resources i-1234567890abcdef0 `  
  --tags 'Key=\\"[Group]\\"",Value=test'
```

Descrever recursos marcados com tags

Os exemplos a seguir mostram como usar filtros com **describe-instances** para visualizar instâncias com tags específicas. Todos os comandos “describe” do EC2 usam essa sintaxe para filtrar por tag em um único tipo de recurso. Como alternativa, é possível usar o comando **describe-tags** para filtrar por tag entre os tipos de recursos do EC2.

Example Exemplo: descreva as instâncias com a chave de tags especificada

O comando a seguir descreve as instâncias com a tag **Stack**, independentemente do valor da tag.

```
aws ec2 describe-instances \  
  --filters Name=tag-Stack,Values=
```

```
--filters Name=tag-key,Values=Stack
```

Example Exemplo: descreva as instâncias com a tag especificada

O comando a seguir descreve as instâncias com a tag **Stack=production**.

```
aws ec2 describe-instances \  
--filters Name=tag:Stack,Values=production
```

Example Exemplo: descreva as instâncias com o valor de tag especificado

O comando a seguir descreve as instâncias com uma tag com o valor **production**, independentemente da chave da tag.

```
aws ec2 describe-instances \  
--filters Name=tag-value,Values=production
```

Example Exemplo: descrever todos os recursos do EC2 com a tag especificada

O comando a seguir descreve todos os recursos do EC2 com a tag **Stack=Test**.

```
aws ec2 describe-tags \  
--filters Name=key,Values=Stack Name=value,Values=Test
```

Adicionar tags a um recurso usando o CloudFormation

Com tipos de recursos do Amazon EC2, você especifica tags usando uma propriedade Tags ou TagSpecifications.

Os exemplos a seguir adicionam a tag **Stack=Production** ao [AWS#EC2#Instance](#) usando a propriedade Tags.

Example Exemplo: tags em YAML

```
Tags:  
- Key: "Stack"  
  Value: "Production"
```

Example Exemplo: tags em JSON

```
"Tags": [  
  {  
    "Key": "Stack",  
    "Value": "Production"  
  }  
]
```

Os exemplos a seguir adicionam a tag **Stack=Production** ao [AWS::EC2::LaunchTemplate](#) [LaunchTemplateData](#) usando a propriedade TagSpecifications.

Example Exemplo: TagSpecifications em YAML

```
TagSpecifications:
```

```
- ResourceType: "instance"
Tags:
- Key: "Stack"
  Value: "Production"
```

Example Exemplo: TagSpecifications em JSON

```
"TagSpecifications": [
  {
    "ResourceType": "instance",
    "Tags": [
      {
        "Key": "Stack",
        "Value": "Production"
      }
    ]
  }
]
```

Cotas de serviço do Amazon EC2

O Amazon EC2 fornece recursos diferentes que você pode usar. Esses recursos incluem imagens, instâncias, volumes e snapshots. Ao criar sua conta da AWS, definimos cotas padrão (também conhecidas como limites) nesses recursos de acordo com a região. Por exemplo, há um limite no número máximo de instâncias que podem ser iniciadas em uma região. Assim, se for necessário executar uma instância na região Oeste dos EUA (Oregon), por exemplo, a solicitação não deverá fazer com que o uso exceda o número máximo de instâncias nessa região.

O console do Amazon EC2 fornece informações de limite para os recursos gerenciados pelos consoles do Amazon EC2 e da Amazon VPC. É possível solicitar o aumento de muitos desses limites. Use as informações de limite que fornecemos para gerenciar sua infraestrutura da AWS. Planeje a solicitação de aumentos dos limites com antecedência antes que sejam necessários.

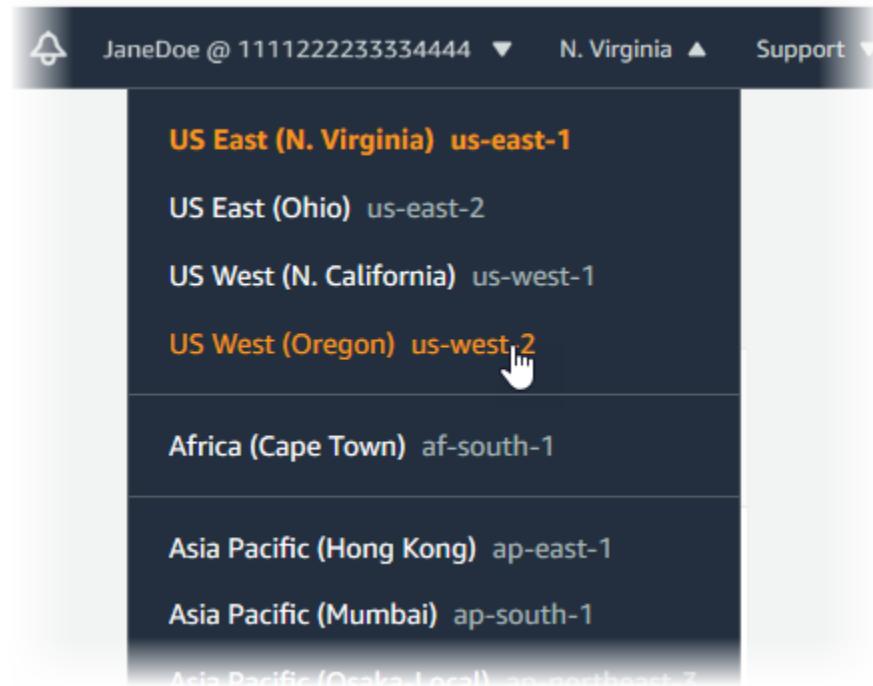
Para obter mais informações, consulte [Endpoints e cotas do Amazon EC2](#) na Referência geral do Amazon Web Services. Para obter informações sobre cotas do Amazon EBS, consulte [Cotas do Amazon EBS \(p. 1490\)](#).

Visualizar os limites atuais

Use a página Limits (Limites) no console do Amazon EC2 para visualizar os limites atuais dos recursos fornecidos pelo Amazon EC2 e pela Amazon VPC, por região.

Como visualizar os limites atuais

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione uma região.



3. Na página de navegação, escolha Limites.
4. Encontre o recurso na lista. Você pode usar os campos de busca para filtrar a lista por nome de recurso ou grupo de recurso. A coluna Current limit (Limite atual) exibe o máximo atual desse recurso para sua conta.

Solicitar um aumento

Use a página Limits (Limites) no console do Amazon EC2 para solicitar um aumento em seus recursos da Amazon VPC ou do Amazon EC2, por região.

Como alternativa, solicite um aumento usando Service Quotas. Para obter mais informações, consulte [Solicitar um aumento de cota](#) no Manual do usuário do Service Quotas.

Como solicitar um aumento usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Na barra de navegação, selecione uma região.
3. Na página de navegação, escolha Limites.
4. Selecione o recurso na lista e escolha Request limit increase (Solicitar aumento de limite).
5. Preencha os campos obrigatórios no formulário de aumento de limite e escolha Submit (Enviar). Responderemos usando o método de contato que você especificou.

Restrição para e-mails enviados usando a porta 25

Em todas as instâncias, o Amazon EC2 restringe o tráfego na porta 25 por padrão. É possível solicitar que essa restrição seja removida. Para obter mais informações, consulte [How do I remove the restriction on port 25 from my EC2 instance \(Como remover a restrição da porta 25 na minha instância do EC2?\)](#) na Central de Conhecimento da AWS.

Relatórios de uso do Amazon EC2

A AWS fornece uma ferramenta de geração de relatório gratuita, chamada AWS Cost Explorer, que permite analisar o custo e o uso das instâncias do EC2 e uso das instâncias reservadas. É possível visualizar dados dos últimos 13 meses e prever o provável valor que você gastará nos próximos três meses. É possível usar o Cost Explorer para ver padrões de gastos de recursos da AWS ao longo do tempo, identificar áreas que precisam de uma investigação mais profunda e ver tendências que você pode usar para entender seus custos. Também é possível especificar os períodos dos dados e visualizar os dados de tempo por dia ou mês.

Veja um exemplo de algumas das perguntas que você pode responder ao usar o Cost Explorer:

- Quanto estou gastando em instâncias de cada tipo?
- Quantas horas de instância estão sendo usadas por um departamento específico?
- Como meu uso de instância é distribuído por zonas de disponibilidade?
- Como meu uso de instância é distribuído pelas contas da AWS?
- Até que ponto estou aproveitando bem minhas Instâncias reservadas?
- Minhas Instâncias reservadas estão me ajudando a economizar?

Para obter mais informações sobre como trabalhar com relatórios no Cost Explorer, incluindo como salvar relatórios, consulte [Analisa os custos com o Cost Explorer](#).

Solução de problemas de instâncias Windows do EC2

Os seguintes procedimentos e dicas podem ajudar a solucionar problemas com suas instâncias Windows do Amazon EC2.

Tópicos

- [Solucionar problemas de execução de instâncias \(p. 1570\)](#)
- [Solução de problemas para conexão à instância do Windows \(p. 1573\)](#)
- [Solucionar problemas de uma instância não acessível \(p. 1581\)](#)
- [Redefinir uma senha de administrador do Windows perdida ou expirada \(p. 1590\)](#)
- [Solução de problemas na interrupção da instância \(p. 1602\)](#)
- [Solucionar problemas de encerramento \(desativação\) da instância \(p. 1605\)](#)
- [Solucionar problemas do Sysprep \(p. 1605\)](#)
- [Usar o EC2Rescue for Windows Server \(p. 1606\)](#)
- [EC2 Serial Console para instâncias do Windows \(p. 1618\)](#)
- [Enviar uma interrupção para diagnóstico \(para usuários avançados\) \(p. 1633\)](#)
- [Problemas comuns com instâncias do Windows \(p. 1634\)](#)
- [Mensagens comuns na solução de problemas de instâncias Windows \(p. 1638\)](#)

Para obter informações adicionais para solucionar problemas com sua instância, use [Usar o EC2Rescue for Windows Server \(p. 1606\)](#). Para obter informações sobre como solucionar problemas com drivers PV, consulte [Solucionar problemas de drivers PV \(p. 571\)](#).

Solucionar problemas de execução de instâncias

Os problemas a seguir impedem que você execute uma instância.

Problemas de execução

- [Limite de instâncias excedido \(p. 1570\)](#)
- [Capacidade insuficiente da instância \(p. 1571\)](#)
- [A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis. \(p. 1571\)](#)
- [A instância é encerrada imediatamente \(p. 1572\)](#)
- [Alto uso de CPU logo após o início do Windows \(p. 1573\)](#)

Limite de instâncias excedido

Description

Você obtém o erro `InstanceLimitExceeded` ao tentar executar uma nova instância ou reiniciar uma instância interrompida.

Cause

Se obtiver um erro `InstanceLimitExceeded` ao tentar executar uma nova instância ou reiniciar uma instância interrompida, isso significa que atingiu o limite do número de instâncias que você pode executar em uma região. Ao criar uma conta da AWS, definimos limites padrão para o número de instâncias que você pode executar por região.

Solution

Você pode solicitar um aumento de limite de instâncias por região. Para obter mais informações, consulte [Cotas de serviço do Amazon EC2 \(p. 1567\)](#).

Capacidade insuficiente da instância

Description

Você obtém o erro `InsufficientInstanceCapacity` ao tentar executar uma nova instância ou reiniciar uma instância interrompida.

Cause

Se você receber esse erro ao tentar executar uma instância ou reiniciar uma instância interrompida, isso significa que, no momento, a AWS não tem capacidade sob demanda suficiente para atender à sua solicitação.

Solution

Para resolver esse problema, experimente o seguinte:

- Espere alguns minutos e envie uma solicitação novamente; a capacidade pode mudar com frequência.
- Envie uma solicitação nova com um número de instâncias reduzido. Por exemplo, se você estiver fazendo uma única solicitação para executar 15 instâncias, tente fazer 3 solicitações para 5 instâncias, ou 15 solicitações de 1 instância.
- Se você estiver executando uma instância, envie uma nova solicitação sem especificar uma zona de disponibilidade.
- Se você estiver executando uma instância, envie uma solicitação nova usando um tipo de instância diferente (que você pode redimensionar posteriormente). Para obter mais informações, consulte [Alterar o tipo de instância \(p. 244\)](#).
- Se você estiver executando instâncias em um placement group de cluster, é possível obter um erro de capacidade insuficiente. Para obter mais informações, consulte [Regras e limitações do placement group \(p. 1047\)](#).

**A configuração solicitada não é suportada atualmente.
Verifique a documentação quanto às configurações compatíveis.**

Description

Você obtém o erro `Unsupported` ao tentar executar uma nova instância porque a configuração da instância não é compatível.

Cause

A mensagem de erro fornece detalhes adicionais. Por exemplo, é possível que um tipo de instância ou opção de compra de instância não seja compatível com a Região ou Zona de Disponibilidade especificada.

Solution

Tente uma configuração de instância diferente. Para pesquisar um tipo de instância que atenda aos seus requisitos, consulte [Localizar um tipo de instância do Amazon EC2 \(p. 242\)](#).

A instância é encerrada imediatamente

Description

Sua instância passa do estado `pending` para o estado `terminated`.

Cause

A seguir estão alguns motivos pelos quais a instância pode ser imediatamente encerrada:

- Você excedeu os limites de volume do EBS. Para obter mais informações, consulte [Limites de volumes de instância \(p. 1507\)](#).
- Um snapshot do EBS está corrompido.
- O volume raiz do EBS está criptografado e você não tem permissões para acessar a Chave do KMS para descriptografia.
- Um snapshot especificado no mapeamento de dispositivo de blocos para a AMI está criptografado e você não tem permissões para acessar a Chave do KMS para descriptografia ou não tem acesso à Chave do KMS para criptografar os volumes restaurados.
- A AMI com armazenamento de instâncias que você usou para executar a instância não tem um item necessário (um arquivo `image.part.xx`).

Para obter mais informações, saiba o motivo do encerramento usando um dos métodos a seguir.

Para obter o motivo do encerramento usando o console do Amazon EC2

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instâncias e selecione a instância.
3. Na primeira guia, encontre o motivo ao lado de State transition reason (Motivo de transição de estado).

Para obter o motivo do encerramento usando a AWS Command Line Interface

1. Use o comando `describe-instances` e especifique o ID da instância.

```
aws ec2 describe-instances --instance-id instance_id
```

2. Revise a resposta JSON retornada pelo comando e observe os valores no elemento de resposta `StateReason`.

O bloco de código a seguir mostra um exemplo de elemento de resposta `StateReason`:

```
"StateReason": {  
    "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",  
    "Code": "Server.InternalError"  
},
```

Como saber o motivo do encerramento usando a AWS CloudTrail

Para obter mais informações, consulte [Viewing events with CloudTrail event history](#) (Visualizar eventos com o histórico de eventos CloudTrail) no AWS CloudTrail User Guide (Guia do usuário do AWS CloudTrail).

Solution

Dependendo do motivo do encerramento, execute uma das seguintes ações:

- **Client.VolumeLimitExceeded: Volume limit exceeded** — exclua volumes não utilizados. É possível [enviar uma solicitação](#) para aumentar seu limite de volume.
- **Client.InternalError: Client error on launch**: verifique se você tem as permissões necessárias para acessar as AWS KMS keys usadas para descriptografar e criptografar volumes. Para obter mais informações, consulte [Using key policies in AWS KMS](#) (Usar políticas de chaves no AWS Key Management Service) no AWS Key Management Service Developer Guide (Guia do desenvolvedor do AWS Key Management Service).

Alto uso de CPU logo após o início do Windows

Se o Windows Update for definido como Verificar se há atualizações, mas permitir que eu escolha fazer download e instalá-las (a configuração de instância padrão), essa verificação poderá consumir entre 50 e 99% da CPU na instância. Se esse consumo de CPU causar problemas para seus aplicativos, você poderá alterar manualmente as configurações do Windows Update no Painel de controle ou usar o seguinte script no campo de dados de usuário do Amazon EC2:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Quando você executar esse script, especifique um valor para /d. O valor padrão é 3. Os valores possíveis incluem o seguinte:

1. Nunca verificar se há atualizações
2. Verificar se há atualizações, mas permitir que eu escolha fazer download e instalá-las
3. Fazer download de atualizações, mas permitir que eu escolha fazer download e instalá-las
4. Instalar atualizações automaticamente

Depois de modificar os dados do usuário para sua instância, você poderá executá-la. Para obter mais informações, consulte [Visualizar e atualizar os dados do usuário da instância \(p. 619\)](#) e [Execução de dados do usuário \(p. 616\)](#).

Solução de problemas para conexão à instância do Windows

A seguir estão os possíveis problemas você pode ter e mensagens de erro que você poderá ver ao tentar se conectar à sua instância do Windows.

Tópicos

- [O Remote Desktop não pode se conectar ao computador remoto \(p. 1574\)](#)
- [Erro ao usar o cliente RDP do macOS \(p. 1576\)](#)
- [O RDP exibe uma tela preta em vez da área de trabalho \(p. 1577\)](#)

- [Não foi possível fazer login remotamente em uma instância com uma conta de usuário que não é de administrador \(p. 1577\)](#)
- [Resolução de problemas do desktop remoto usando o AWS Systems Manager \(p. 1577\)](#)
- [Habilitar a área de trabalho remota em uma instância do EC2 com registro remoto \(p. 1580\)](#)

O Remote Desktop não pode se conectar ao computador remoto

Tente o seguinte para resolver problemas relacionados à conexão com sua instância:

- Verifique se você está usando o nome de host DNS público correto. No console do Amazon EC2, selecione a instância e verifique o DNS público (IPv4) no painel de detalhes. Se sua instância estiver em uma VPC e você não vir um nome DNS público, deverá habilitar nomes de host DNS. Para obter mais informações, consulte [Usar DNS com a VPC](#), no Guia do usuário da Amazon VPC.
- Verifique se sua instância tem um endereço IPv4 público. Se não tiver, associe um endereço IP elástico à sua instância. Para obter mais informações, consulte [Endereços IP elásticos \(p. 993\)](#).
- Para conectar-se à sua instância usando um endereço IPv6, verifique se seu computador local tem um endereço IPv6 e está configurado para usar IPv6. Se você executou uma instância a partir de uma AMI do Windows Server 2008 SP2 ou anteriormente, sua instância não estará configurada automaticamente para reconhecer um endereço IPv6 atribuído à instância. Para obter mais informações, consulte [Configurar o IPv6 em suas instâncias](#) no Guia do usuário da Amazon VPC.
- Verifique se o security group tem uma regra que permita o acesso RDP. Para obter mais informações, consulte [Crie um grupo de segurança \(p. 7\)](#).
- Se você copiou a senha, mas obtiver o erro `Your credentials did not work`, tente digitá-la manualmente quando solicitado. É possível que você tenha omitido um caractere ou inserido um espaço em branco extra ao copiar a senha.
- Verifique se a instância passou nas verificações de status. Para obter mais informações, consulte [Verificações de status para as instâncias \(p. 867\)](#) e [Solução de problemas em instâncias com verificações de status que apresentam falha](#) (Guia do usuário do Amazon EC2 para instâncias do Linux).
- Verifique se a tabela de rotas da sub-rede tem uma rota que envie todo o tráfego destinado para fora da VPC para o gateway da Internet da VPC. Para obter mais informações, consulte [Criação de uma tabela de rotas personalizada](#) (gateways da Internet) no Guia do usuário da Amazon VPC.
- Verifique se o Firewall do Windows ou outros softwares de firewall não estão bloqueando o tráfego de RDP para a instância. Recomendamos que você desabilite o Firewall do Windows e controle o acesso à sua instância usando regras de security group. Você pode usar [AWSSupport-TroubleshootRDP \(p. 1577\)](#) para [disable the Windows Firewall profiles using SSM Agent](#). Para desabilitar o Firewall do Windows em uma instância do Windows que não esteja configurada para o AWS Systems Manager, use [AWSSupport-ExecuteEC2Rescue \(p. 1579\)](#), ou use as seguintes etapas manuais:

Etapas manuais

1. Interrompa a instância afeta e desanexe seu volume raiz.
2. Execute uma instância temporária na mesma zona de disponibilidade que a instância afetada.

Warning

Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas adicionais ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco. Como alternativa, selecione uma AMI diferente para a instância temporária. Por exemplo, se a instância original

usar a AMI Windows da AWS para Windows Server 2008 R2, execute a instância temporária usando uma AMI Windows da AWS para Windows Server 2012.

3. Anexe o volume raiz da instância afetada a essa instância temporária. Conecte-se à instância temporária, abra o utilitário Disk Management e ative a unidade.
4. Abra Regedit e selecione HKEY_LOCAL_MACHINE. No menu Arquivo, escolha Carregar Hive. Selecione a unidade, abra o arquivo Windows\System32\config\SYSTEM e especifique um nome de chave quando solicitado (você pode usar qualquer nome).
5. Selecione a chave que você acabou de carregar e vá até ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy. Para cada chave com um nome da forma xxxxProfile, selecione a chave e altere EnableFirewall de 1 a 0. Selecione a chave novamente e, no menu Arquivo, escolha Descarregar Hive.
6. (Opcional) Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas a seguir ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco.

Warning

O procedimento a seguir descreve como editar o Registro do Windows usando o Editor do Registro. Se você não estiver familiarizado com o Registro do Windows ou como fazer alterações com segurança usando o Editor do Registro, consulte[Configure the Registry](#) (Configurar o Registro).

- a. Abra um prompt de comando, digite regedit.exe e pressione Enter.
- b. No Editor do Registro, escolha HKEY_LOCAL_MACHINE no menu contextual (clique com o botão direito do mouse), depois escolha Localizar.
- c. Digite Windows Boot Manager e escolha Localizar Próxima.
- d. Escolha a chave chamada 11000001. Essa chave é irmã da chave que você localizou na etapa anterior.
- e. No painel direito, selecione Element e escolha Modificar no menu de contexto (clique com o botão direito do mouse).
- f. Localize a assinatura de disco de quatro bytes no deslocamento 0x38 nos dados. Inverta os bytes para criar a assinatura de disco e anote-a. Por exemplo, a assinatura de disco representada pelos seguintes dados é E9EB3AA5:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

- g. Em uma janela do prompt de comando, execute o comando a seguir para iniciar o Microsoft DiskPart.

```
diskpart
```

- h. Execute o comando DiskPart a seguir para selecionar o volume. (Você pode verificar se o número do disco é 1 usando o utilitário Gerenciamento de disco.)

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

- i. Execute o comando DiskPart a seguir para obter a assinatura do disco.

```
DISKPART> uniqueid disk
```

Disk ID: **0C764FA8**

- j. Se a assinatura de disco mostrada na etapa anterior não corresponder à assinatura de disco do BCD que você anotou anteriormente, use o seguinte comando DiskPart para alterar a assinatura de disco para que ela corresponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

7. Usando o utilitário Disk Management, desative o volume da unidade.

Note

A unidade ficará offline automaticamente se a instância temporária estiver executando o mesmo sistema operacional que a instância afetada, portanto, você não precisará deixá-la offline manualmente.

8. Desanexe o volume da instância temporária. Você pode encerrar a instância temporária se você não tiver utilização adicional para ela.
9. Restaure o volume raiz da instância afetada anexando-a como /dev/sda1.
10. Inicie a instância.
 - Verifique se a autenticação no nível de rede está desabilitada nas instâncias que não fazem parte de um domínio do Active Directory (use [AWSSupport-TroubleshootRDP \(p. 1577\)](#) para [disable NLA](#)).
 - Verifique se o tipo de inicialização do serviço da área de trabalho remota (TermService) é automático e se o serviço foi iniciado (use [AWSSupport-TroubleshootRDP \(p. 1577\)](#) para [enable and start the RDP service](#)).
 - Verifique se você está se conectando à porta correta do protocolo RDP, que por padrão é 3389 (use [AWSSupport-TroubleshootRDP \(p. 1577\)](#) para [read the current RDP port](#) e [change it back to 3389](#)).
 - Verifique se as conexões da área de trabalho remota são permitidas na sua instância (use [AWSSupport-TroubleshootRDP \(p. 1577\)](#) para [enable Remote Desktop connections](#)).
 - Verifique se a senha não expirou. Se a senha expirou, você poderá redefini-la. Para obter mais informações, consulte [Redefinir uma senha de administrador do Windows perdida ou expirada \(p. 1590\)](#).
 - Se você tentar conectar-se usando uma conta de usuário que você criou na instância e receber o erro *The user cannot connect to the server due to insufficient access privileges*, verifique se você concedeu ao usuário o direito de fazer login localmente. Para obter mais informações, consulte [Conceder o direito de fazer login localmente a um membro](#).
 - Se você tentar mais sessões simultâneas do RDP do que o máximo permitido, sua sessão será encerrada com a mensagem *Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost*. Por padrão, são permitidas duas sessões simultâneas do RDP para sua instância.

Erro ao usar o cliente RDP do macOS

Se você estiver se conectando a uma instância do Windows Server 2012 R2 usando o cliente de Conexão com a Área de Trabalho Remota do site da Microsoft, você pode obter o seguinte erro:

```
Remote Desktop Connection cannot verify the identity of the computer that you want to connect to.
```

Faça download do aplicativo Área de Trabalho Remota da App Store do Max e use o aplicativo para conectar-se à instância.

O RDP exibe uma tela preta em vez da área de trabalho

Tente o seguinte para resolver esse problema:

- Verifique a saída do console para ver se há informações adicionais. Para obter a saída do console da instância usando o console do Amazon EC2, selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema).
- Verifique se você está executando a versão mais recente do cliente do RDP.
- Tente as configurações padrão para o cliente do RDP. Para obter mais informações, consulte [Ambiente de sessão remota](#).
- Se você estiver usando o Remote Desktop Connection, tente iniciá-lo com a opção /admin da seguinte forma.

```
mstsc /v:instance /admin
```

- Se o servidor estiver executando um aplicativo de tela total, talvez tenha parado de responder. Use Ctrl +Shift+Esc para iniciar o Windows Task Manager e feche o aplicativo.
- Se o servidor for utilizado em excesso, talvez tenha parado de responder. Para monitorar a instância usando o console do Amazon EC2, selecione a instância e escolha a guia Monitoramento. Se você precisar alterar o tipo de instância para um tamanho maior, consulte [Alterar o tipo de instância \(p. 244\)](#).

Não foi possível fazer login remotamente em uma instância com uma conta de usuário que não é de administrador

Se você não puder participar remotamente em uma instância do Windows com uma conta de usuário que não tenha uma conta de administrador, conceda ao usuário o direito de entrada localmente. Veja [Dar a um usuário ou grupo o direito de entrar localmente nos controladores de domínio no domínio](#).

Resolução de problemas do desktop remoto usando o AWS Systems Manager

Você pode usar o AWS Systems Manager para resolver problemas conectando-se à sua instância do Windows usando RDP.

AWSSupport-TroubleshootRDP

O documento de automação AWSSupport-TroubleshootRDP permite ao usuário verificar ou modificar configurações comuns na instância de destino que possam afetar as conexões RDP (Remote Desktop Protocol), como os perfis RDP Port, Network Layer Authentication (NLA) e Windows Firewall. Por padrão, o documento lê e exibe os valores dessas configurações.

O documento de automação AWSSupport-TroubleshootRDP pode ser usado com instâncias do EC2, instâncias locais e máquinas virtuais (VMs) habilitadas para uso com o AWS Systems Manager (instâncias gerenciadas). Além disso, ele também pode ser usado com instâncias do EC2 para Windows Server não habilitadas para uso com o Systems Manager. Para obter informações sobre a ativação de instâncias para uso com o AWS Systems Manager, consulte [AWS Systems Manager Managed Instances](#) (Instâncias

gerenciadas do AWS Systems Manager) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).

Para resolver os problemas usando o documento AWSSupport-TroubleshootRDP

1. Faça login no [console do Systems Manager](#).
2. Verifique se você está na mesma região que a instância prejudicada.
3. Abra o documento [AWSSupport-TroubleshootRDP](#).
4. Em Execution Mode (Modo de execução), escolha Simple execution (Execução simples).
5. Em Input parameters (Parâmetros de entrada), InstanceId, ative Show interactive instance picker (Mostrar seletor interativo de instâncias).
6. Escolha a instância do Amazon EC2.
7. Revise os [exemplos \(p. 1578\)](#) e escolha Execute (Executar).
8. Para monitorar o progresso da execução, no Execution status (Status execução), aguarde o status mudar de Pending (Pendente) para Success (Êxito). Expanda Outputs (Saídas) para visualizar os resultados. Para visualizar a saída de etapas individuais, Executed Steps (Etapas executadas), escolha um item da Step ID (ID da etapa).

Exemplos do AWSSupport-TroubleshootRDP

Os exemplos a seguir mostram como conquistar tarefas de resolução de problema comuns usando AWSSupport-TroubleshootRDP. Você pode usar o comando de exemplo da AWS CLI [start-automation-execution](#) ou o link fornecido para o AWS Management Console.

Example Exemplo: verifique o status atual de RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --parameters "InstanceId=instance_id" --region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Exemplo: desativar o Firewall do Windows

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --parameters "InstanceId=instance_id,Firewall=Disable" --region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Exemplo: desativar a autenticação no nível da rede

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --  
parameters "InstanceId=instance_id,NLASettingAction=Disable" --region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-  
TroubleshootRDP?region=region_code#documentVersion
```

Example Exemplo: definir o tipo de inicialização do serviço RDP como automático e iniciar o serviço RDP

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --  
parameters "InstanceId=instance_id,RDPServiceStartupType=Auto, RDPServiceAction=Start" --  
region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/  
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=  
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Exemplo: restaurar a porta RDP padrão (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --  
parameters "InstanceId=instance_id,RDPPortAction=Modify" --region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-  
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example Example: permitir conexões remotas

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --  
parameters "InstanceId=instance_id,RemoteConnections=Enable" --region region_code
```

AWS Systems ManagerConsole do :

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-  
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport-ExecuteEC2Rescue

O documento de automação AWSSupport-ExecuteEC2Rescue usa [Usar o EC2Rescue for Windows Server \(p. 1606\)](#) para solucionar e restaurar automaticamente problemas de conectividade e RDP na

instância do EC2. Para obter mais informações, consulte [Executar a ferramenta EC2Rescue em instâncias inacessíveis](#).

O documento de automação AWSSupport-ExecuteEC2Rescue exige que a instância seja interrompida e reiniciada. O Systems Manager Automation interrompe a instância e cria uma Imagem de máquina da Amazon (AMI). Dados armazenados nos volumes de armazenamento da instância são perdidos. O endereço IP público será alterado se você não estiver usando um endereço IP elástico. Para obter mais informações, consulte [Run the EC2Rescue Tool on Unreachable Instances](#) (Executar a ferramenta EC2Rescue em instâncias inacessíveis) no AWS Systems Manager User Guide (Guia do usuário do AWS Systems Manager).

Para resolver o problema usando o documento AWSSupport-ExecuteEC2Rescue

1. Abra o [console do Systems Manager](#).
2. Verifique se você está na mesma região que a instância Amazon EC2 prejudicada.
3. Abra o documento [AWSSupport-ExecuteEC2Rescue](#).
4. Em Execution Mode (Modo de execução), escolha Simple execution (Execução simples).
5. Na seção Input parameters (Parâmetros de entrada), em UnreachableInstanceId, insira o ID da instância do Amazon EC2 para a instância inacessível.
6. (Opcional) Para LogDestination, insira o nome do bucket do Amazon Simple Storage Service (Amazon S3) se quiser coletar logs do sistema operacional para solucionar problemas da sua instância do Amazon EC2. Os logs são enviados automaticamente para o bucket especificado.
7. Selecione Execute (Executar).
8. Para monitorar o progresso da execução, no status Execution (Execução), aguarde o status mudar de Pending (Pendente) para Success (Concluído com sucesso). Expanda Outputs (Saídas) para visualizar os resultados. Para visualizar a saída de etapas individuais, Executed Steps (Etapas executadas), escolha Step ID (ID da etapa).

Habilitar a área de trabalho remota em uma instância do EC2 com registro remoto

Se a instância inacessível não for gerenciada pelo Gerenciador de sessões do AWS Systems Manager, você poderá usar o registro remoto para habilitar a área de trabalho remota.

1. No console do EC2, interrompa a instância inacessível.
2. Anexe o volume raiz da instância inacessível a outra instância na mesma zona de disponibilidade.
3. Na instância à qual você anexou o volume raiz, abra o Gerenciamento de disco. Para abrir o Gerenciamento de disco, execute

```
diskmgmt.msc
```

4. Clique com o botão direito do mouse no volume raiz da instância afetada e escolha Online.
5. Abra o Editor do Registro do Windows executando o seguinte comando:

```
regedit
```

6. Na árvore de console do Editor do Registro, escolha HKEY_LOCAL_MACHINE e selecione File (Arquivo)>Load Hive (Carregar hive).
7. Selecione a unidade do volume conectado, navegue até \Windows\System32\config\, SYSTEM, selecione e escolha Open (Abrir).
8. Em Key Name (Nome da chave), insira um nome exclusivo para o hive e escolha OK.

9. Faça uma cópia de backup do hive do registro antes de fazer qualquer alteração no registro.
 - a. Na árvore de console do Editor do Registro, selecione o hive carregado: HKEY_LOCAL_MACHINE \your key name.
 - b. Escolha File (Arquivo) > Export (Exportar).
 - c. Na caixa de diálogo Export Registry File (Exportar arquivo do registro), escolha o local no qual deseja salvar a cópia de backup e digite um nome para o arquivo de backup no campo File Name (Nome do arquivo).
 - d. Escolha Save (Salvar).
 10. Na árvore do console do Editor do Registro, navegue para HKEY_LOCAL_MACHINE\your key name\ControlSet001\Control\Terminal Server e, depois, no painel de detalhes, clique duas vezes em fDenyTSConnections.
 11. Na caixa de valor Edit DWORD (Editar DWORD) insira 0 no campo Value Data (Dados do valor).
 12. Escolha OK.
- Note
- Se o valor no campo Value data (Dados do valor) for 1, a instância negará conexões de área de trabalho remota. Um valor de 0 permitirá conexões de área de trabalho remota.
13. Feche os consoles do Editor do Registro e do Gerenciamento de disco.
 14. No console do EC2, desanexe o volume raiz da instância à qual você o anexou e anexe-o novamente à instância inacessível. Ao anexar o volume à instância inacessível, insira /dev/sda1 no campo device (dispositivo).
 15. Reinicie a instância inacessível.

Soluçinar problemas de uma instância não acessível

Se você não conseguir alcançar sua instância do Windows via SSH ou RDP, poderá fazer uma captura de tela da sua instância evê-la como imagem. Isso fornece visibilidade quanto ao status da instância e permite uma solução de problemas mais rápida. Também é possível usar o [EC2 Rescue \(p. 1606\)](#) em instâncias executando o Windows Server 2008 ou posterior para coletar e analisar a data de instâncias offline.

- [Obter uma captura de tela de uma instância inacessível \(p. 1581\)](#)
- [Capturas de tela comuns \(p. 1582\)](#)

Para obter informações sobre solução de problemas de uma instância do Linux inacessível, consulte [Soluçinar problemas de uma instância não acessível](#).

Obter uma captura de tela de uma instância inacessível

Você pode obter capturas de tela de uma instância enquanto ela estiver em execução ou após haver falha. Não há custo de transferência de dados para a captura de tela. A imagem é gerada em formato JPG e não é maior que 100 KB. Esse recurso não é compatível quando a instância está usando um driver NVIDIA GRID, está em instâncias bare metal (instâncias do tipo *.meta1) ou é equipada com processadores Graviton ou Graviton 2 baseados em Arm. Este recurso está disponível nas seguintes regiões:

- Região Ásia-Pacífico (Hong Kong)

- Asia Pacific (Tokyo) Region
- Asia Pacific (Seoul) Region
- Asia Pacific (Singapore) Region
- Asia Pacific (Sydney) Region
- Asia Pacific (Mumbai) Region
- US East (N. Virginia) Region
- US East (Ohio) Region
- US West (Oregon) Region
- US West (N. California) Region
- Europe (Ireland) Region
- Europe (Frankfurt) Region
- Região da Europa (Milão)
- Europe (London) Region
- Região Europa (Paris)
- Região Europa (Estocolmo)
- Região Europa (Paris)
- South America (São Paulo) Region
- Canada (Central) Region
- Região Oriente Médio (Bahrein)
- Região da África (Cidade do Cabo)
- Região China (Pequim)
- Região China (Ningxia)

Para obter uma captura de tela de uma instância em execução usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação à esquerda, escolha Instances (Instâncias).
3. Selecione a instância a ser capturada.
4. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get instance screenshot (Obter captura de tela da instância).
5. Escolha Download e clique com o botão direito do mouse na imagem para fazer download e salvá-la.

Para obter uma captura de tela de uma instância em execução usando a linha de comando

Você pode usar um dos comandos a seguir. A saída apresentada é codificado por base64. Para obter mais informações sobre essas interfaces de linha de comando, consulte [Acessar o Amazon EC2 \(p. 3\)](#).

- `get-console-screenshot` (AWS CLI)
- `GetConsoleScreenshot` (API de consulta do Amazon EC2)

Para chamadas de API, o conteúdo apresentado é base64. Para ferramentas de linha de comando, a decodificação é executada para você.

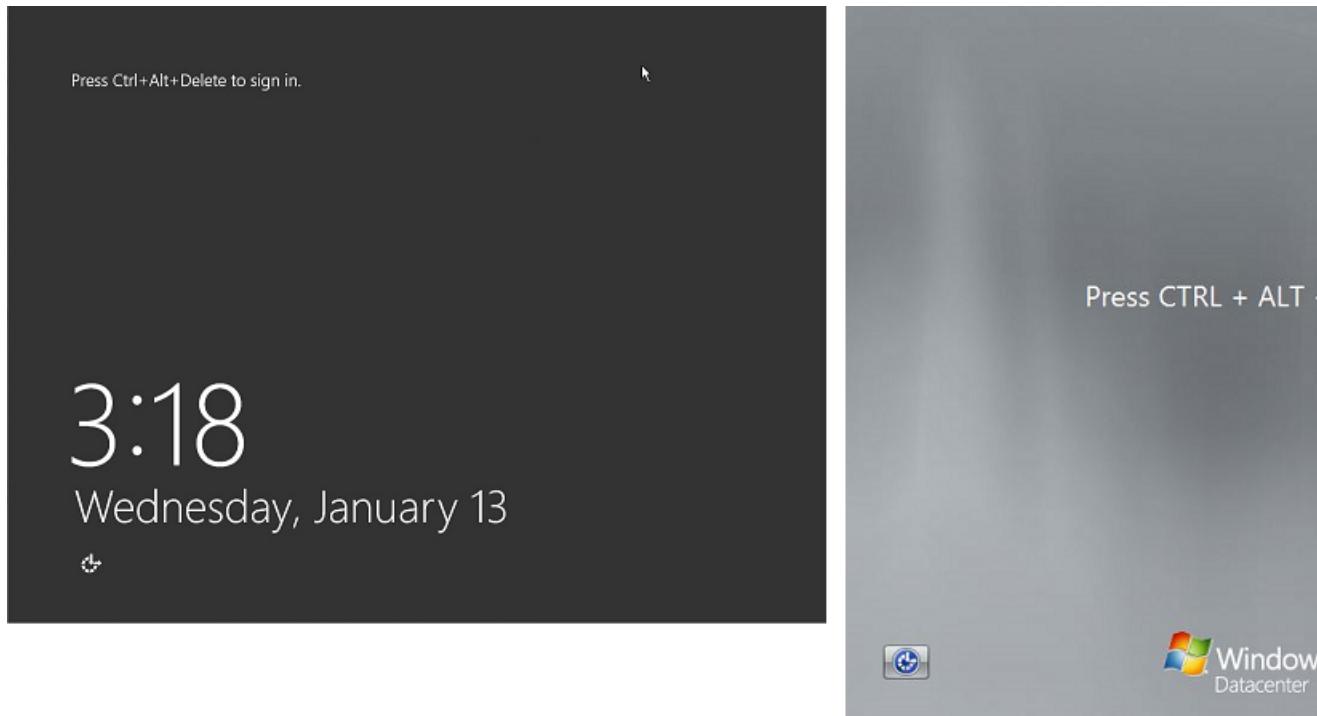
Capturas de tela comuns

Você pode usar as seguintes informações para ajudar a solucionar uma instância inacessível com base nas capturas de tela retornadas pelo serviço.

- Tela de login (Ctrl+Alt+Delete) (p. 1583)
- Tela de console de recuperação (p. 1585)
- Tela do gerenciador de inicialização do Windows (p. 1587)
- Tela Sysprep (p. 1587)
- Tela de preparação (p. 1588)
- Tela do Windows Update (p. 1589)
- Chkdsk (p. 1590)

Tela de login (Ctrl+Alt+Delete)

O serviço de captura de tela de console retornou o seguinte.



Se uma instância se tornar inacessível durante o login, talvez haja um problema com a configuração de rede ou com os Serviços de Área de Trabalho Remota do Windows. Uma instância também poderá não responder se um processo estiver usando grandes quantidades de CPU.

Configuração de rede

Use as seguintes informações para verificar se as configurações da AWS, do Microsoft Windows e da rede local (ou no local) não estão bloqueando o acesso à instância.

Configuração de rede da AWS

Configuração	Verificar
Configuração do security group	Verifique se a porta 3389 está aberta para o security group. Verifique se você está se conectando ao endereço IP público certo. Se a instância não foi associada a um IP elástico, o IP

Configuração	Verificar
	público será alterado depois que a instância for interrompida/iniciada. Para obter mais informações, consulte O Remote Desktop não pode se conectar ao computador remoto (p. 1574) .
Configuração da VPC (Network ACLs)	Verifique se a lista de controle de acesso (ACL) para sua Amazon VPC não está bloqueando acesso. Para obter informações, consulte Network ACLs no Guia do usuário da Amazon VPC.
Configuração de VPN	Se você estiver se conectando à VPC usando uma rede virtual privada (VPN), verifique a conectividade do túnel VPN. Para obter mais informações, consulte Como solucionar problemas de conectividade do túnel VPN para uma Amazon VPC?

Configuração de rede do Windows

Configuração	Verificar
Firewall do Windows	Verifique se o firewall do Windows não está bloqueando as conexões com a sua instância. Desabilite o firewall do Windows como descrito no item 7 da seção sobre solução de problemas do Remote Desktop, O Remote Desktop não pode se conectar ao computador remoto (p. 1574) .
Configuração avançada de TCP/IP (uso de IP estático)	A instância pode não responder porque você configurou um endereço IP estático. Para uma VPC, crie uma interface de rede (p. 1015) e anexe-a à instância (p. 1017) . Para o EC2 Classic, habilite DHCP.

Configuração de rede local ou no local

Verifique se uma configuração de rede local não está bloqueando o acesso. Tente se conectar a uma outra instância na mesma VPC onde se encontra a instância inacessível. Se você não conseguir acessar outra instância, trabalhe com o administrador de rede local para determinar se uma política local está restringindo o acesso.

Problemas com o Remote Desktop Services

Se não for possível acessar a instância durante o login, talvez haja um problema com os Serviços de Área de Trabalho Remota (RDS - Remote Desktop Services) na instância.

Configuração do Remote Desktop Services

Configuração	Verificar
O RDS está em execução	Verifique se o RDS está em execução na instância. Conecte-se à instância usando o snap-in de serviços do Microsoft Management Console (MMC) (<code>services.msc</code>). Na lista de serviços, verifique se o Remote Desktop Services está Running (Em execução). Se não

Configuração	Verificar
	estiver, inicie-o e defina o tipo de inicialização como Automático. Se você não puder se conectar à instância usando o snap-in Services, desanexe o volume raiz da instância, crie um snapshot do volume ou crie uma AMI dele, anexe o volume original a outra instância na mesma zona de disponibilidade como um volume secundário e modifique a chave de Registro Start . Ao terminar, anexe novamente o volume raiz à instância original. Para obter mais informações sobre como desanexar volumes, consulte Desanexar um volume do Amazon EBS de uma instância Windows (p. 1290) .
O RDS está habilitado	Mesmo se o serviço tiver sido iniciado, ele pode estar desabilitado. Desanexe o volume raiz da instância, crie um snapshot do volume ou crie uma AMI dele, anexe o volume original a outra instância na mesma zona de disponibilidade como um volume secundário e habilite o serviço modificando a chave do registro Terminal Server (Servidor de terminal) conforme descrito em Habilitar a área de trabalho remota em uma instância do EC2 com registro remoto (p. 1580) . Ao terminar, anexe novamente o volume raiz à instância original. Para obter mais informações, consulte Desanexar um volume do Amazon EBS de uma instância Windows (p. 1290) .

Alto uso da CPU

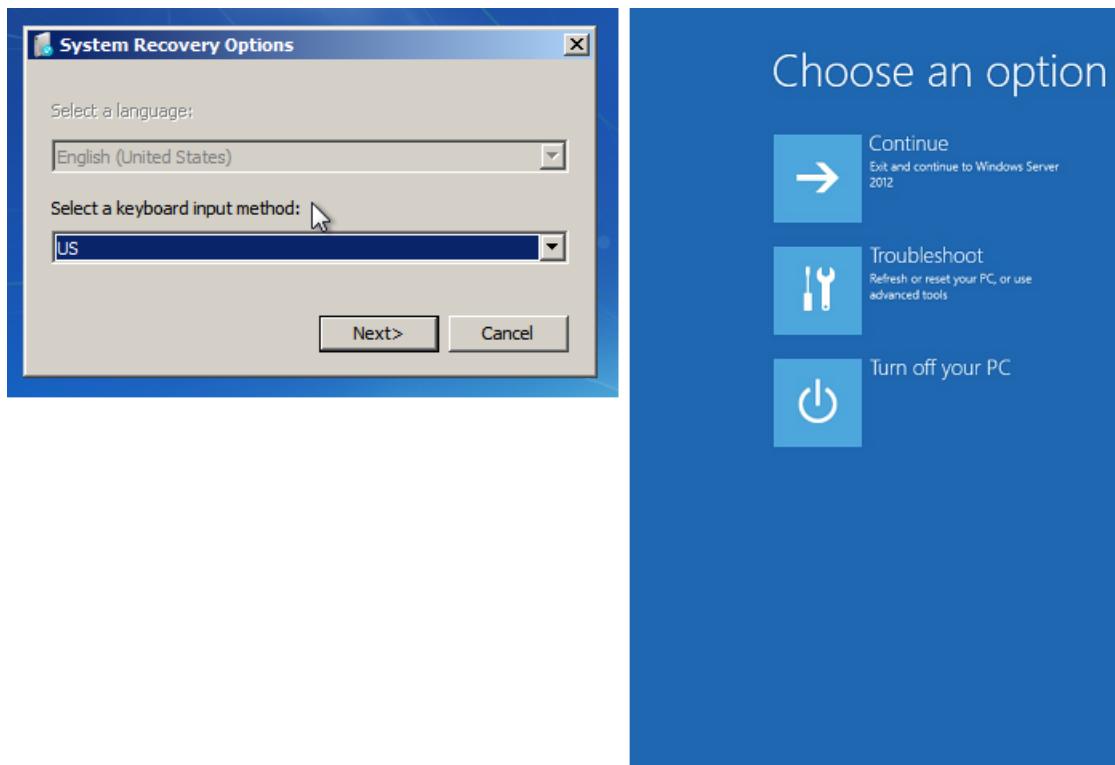
Verifique a métrica CPUUtilization (máximo) em sua instância usando o Amazon CloudWatch. Se CPUUtilization (máximo) for um número alto, aguarde a desativação da CPU e tente se conectar novamente. A utilização elevada da CPU pode ser causada por:

- Atualizações do Windows
- Verificação de software de segurança
- Script de inicialização personalizado
- Programador de tarefas

Para obter mais informações, consulte [Obter as estatísticas de um recurso específico](#) no Guia do usuário do Amazon CloudWatch. Para obter mais dicas sobre solução de problemas, consulte [Alto uso de CPU logo após o início do Windows \(p. 1573\)](#).

Tela de console de recuperação

O serviço de captura de tela de console retornou o seguinte.



O sistema operacional pode ser inicializado no console de recuperação e travar nesse estado se a `bootstatuspolicy` não estiver definida como `ignoreallfailures`. Use o procedimento a seguir para alterar a configuração de `bootstatuspolicy` para `ignoreallfailures`.

Por padrão, a configuração de políticas para AMIs públicas do Windows fornecidas pela AWS é definida como `ignoreallfailures`.

1. Interrompa a instância inacessível.
2. Crie um snapshot de novo volume raiz. O volume raiz é anexado à instância como `/dev/sda1`.

Desanexe o volume raiz da instância inacessível, crie um snapshot do volume ou crie uma AMI dele e anexe-a a outra instância na mesma zona de disponibilidade que um volume secundário. Para obter mais informações, consulte [Desanexar um volume do Amazon EBS de uma instância Windows \(p. 1290\)](#).

Warning

Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas adicionais ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco. Como alternativa, selecione uma AMI diferente para a instância temporária. Por exemplo, se a instância original usar uma AMI para Windows Server 2008 R2, execute a instância temporária usando uma AMI para Windows Server 2012. Se você precisar criar uma instância temporária com base na mesma AMI, consulte a etapa 6 em [O Remote Desktop não pode se conectar ao computador remoto \(p. 1574\)](#) para evitar uma colisão de assinatura de disco.

3. Faça login na instância e execute o seguinte comando a partir de um prompt para alterar a configuração de `bootstatuspolicy` para `ignoreallfailures`:

```
bcdeedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy ignoreallfailures
```

4. Reanexe o volume à instância inacessível e inicie a instância novamente.

Tela do gerenciador de inicialização do Windows

O serviço de captura de tela de console retornou o seguinte.



Windows
cause.

1. In
2. Ch
3. cl

If you
manufac

Fil

Sta

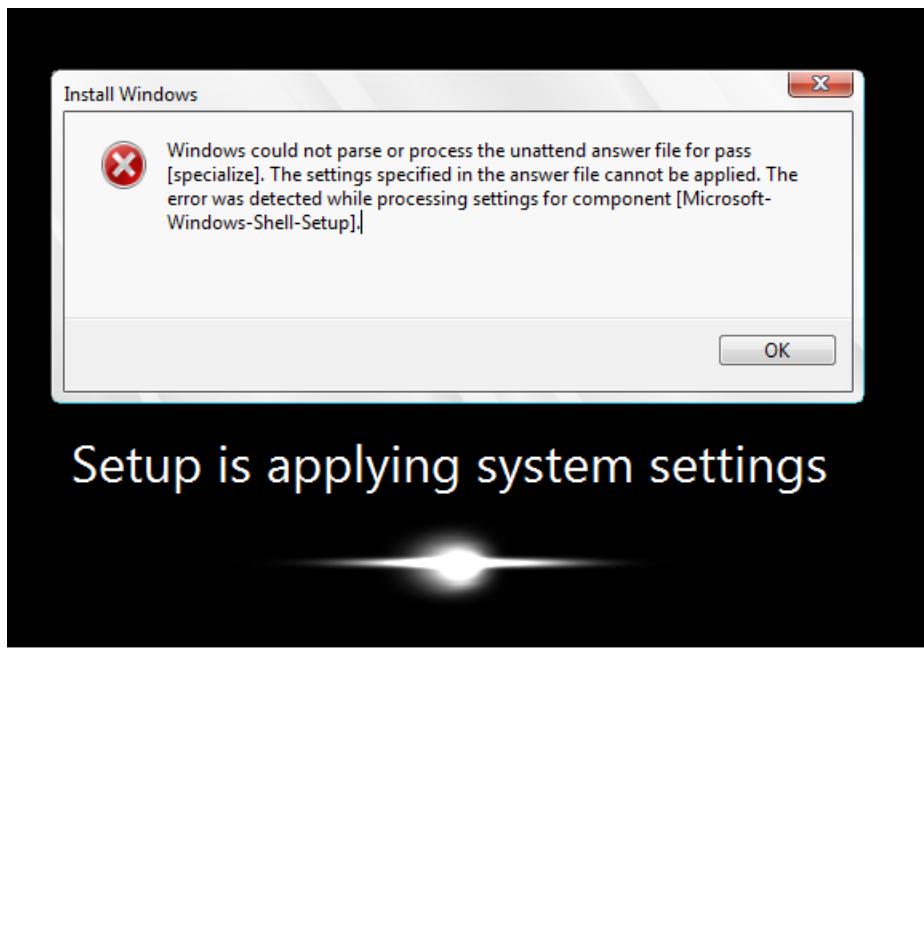
Inf

ENTER=

O sistema operacional experimentou um dano fatal no arquivo de sistema e/ou no Registro. Quando a instância trava nesse estado, você deve recuperá-la de uma AMI de backup recente ou executar uma instância de substituição. Se você precisar acessar dados na instância, desanexe todos os volumes raiz da instância inacessível, crie um snapshot desses volumes ou crie uma AMI deles e anexe-os a outra instância na mesma zona de disponibilidade como um volume secundário. Para obter mais informações, consulte [Desanexar um volume do Amazon EBS de uma instância Windows \(p. 1290\)](#).

Tela Sysprep

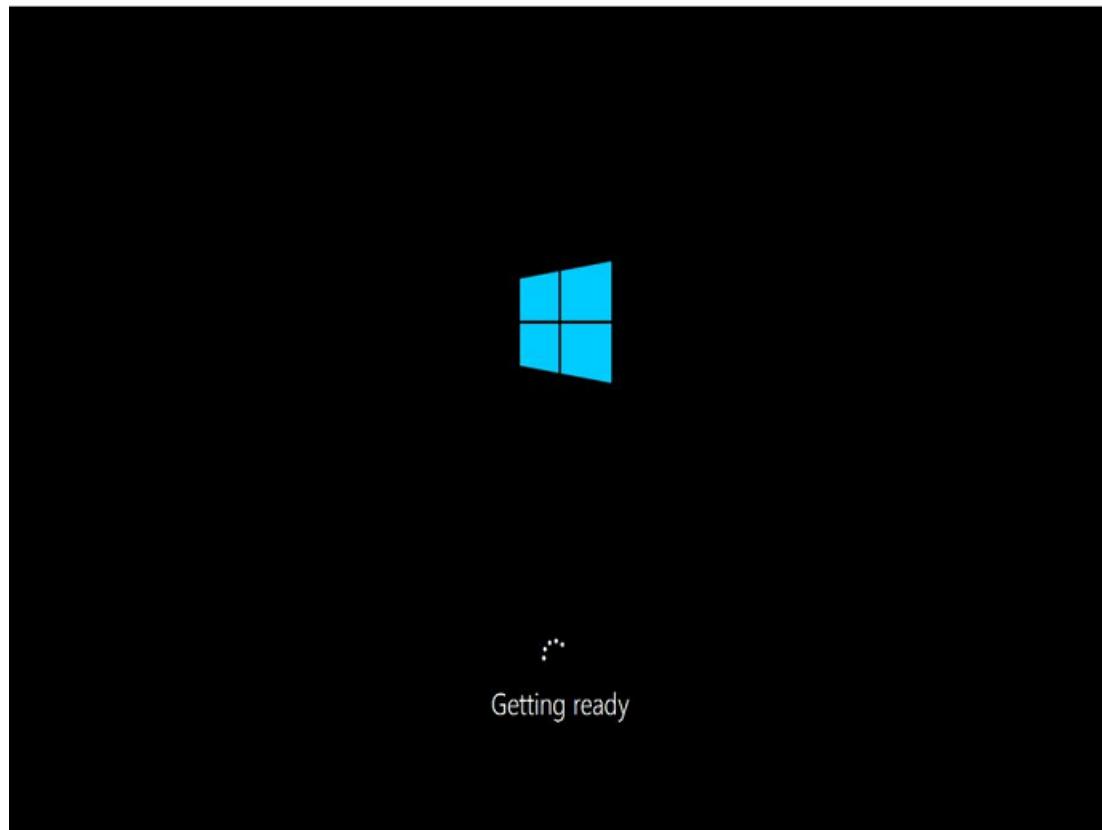
O serviço de captura de tela de console retornou o seguinte.



Você poderá ver essa tela se não tiver usado o EC2Config Service para chamar Sysprep ou se o sistema operacional falhar ao executar o Sysprep. É possível redefinir a senha usando o [EC2Rescue \(p. 1606\)](#). Caso contrário, [Criar uma imagem de máquina da Amazon \(AMI\) padronizada usando o Sysprep \(p. 42\)](#).

Tela de preparação

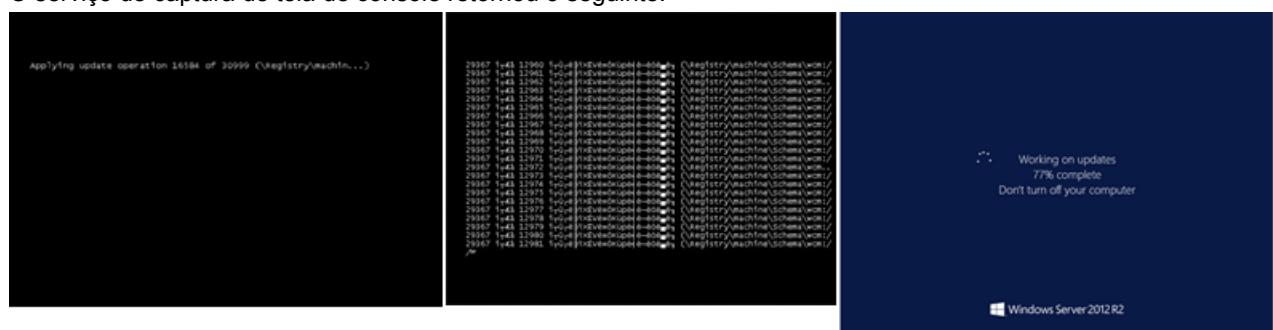
O serviço de captura de tela de console retornou o seguinte.



Atualize o Instance Console Screenshot Service repetidamente para verificar se o anel de andamento está girando. Se o anel estiver girando, aguarde a inicialização do sistema operacional. Você também pode verificar a métrica CPUUtilization (máximo) em sua instância usando o Amazon CloudWatch para ver se o sistema operacional está ativo. Se o anel de andamento não estiver girando, a instância poderá travar no processo de inicialização. Reinicialize a instância. Se a reinicialização não resolver o problema, recupere a instância de uma AMI de backup recente ou execute uma instância de substituição. Se você precisar acessar os dados na instância, desanexe o volume raiz da instância inacessível, crie um snapshot do volume ou crie uma AMI dele. Em seguida, anexe-o a outra instância na mesma zona de disponibilidade que o volume secundário.

Tela do Windows Update

O serviço de captura de tela de console retornou o seguinte.



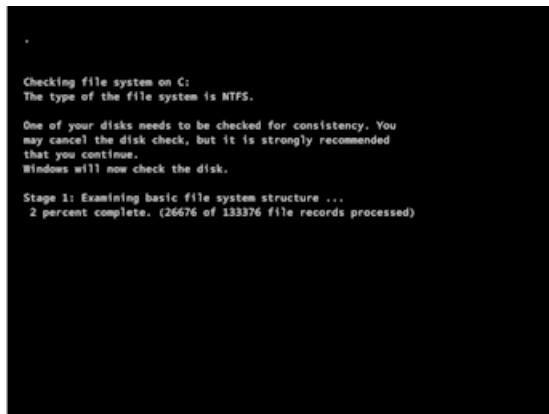
O processo do Windows Update está atualizando o Registro. Aguarde o término da atualização. Não reinicialize nem interrompa a instância, pois isso pode causar danos aos dados durante a atualização.

Note

O processo do Windows Update pode consumir recursos no servidor durante a atualização. Se você tiver esse problema com frequência, considere usar um tipo de instância e volumes do EBS mais rápidos.

Chkdsk

O serviço de captura de tela de console retornou o seguinte.



O Windows está executando a ferramenta de sistema chkdsk na unidade para verificar a integridade do sistema de arquivos e corrigir os erros lógicos do sistema de arquivos. Aguarde a conclusão do processo.

Redefinir uma senha de administrador do Windows perdida ou expirada

Se não conseguir mais acessar sua instância do Amazon EC2 no Windows porque a senha do administrador do Windows está incorreta ou expirou, você poderá redefinir a senha.

Note

Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte [Redefinir senhas e chaves SSH nas instâncias do Amazon EC2](#) no Guia do usuário do AWS Systems Manager.

Os métodos manuais para redefinir a senha de administrador usam o EC2Launch v2, o EC2Config ou o EC2Launch.

- Para todas as AMIs do Windows compatíveis que incluem o serviço EC2Launch v2, use o EC2Launch v2.
- Para AMIs do Windows anteriores ao Windows Server 2016, você pode usar o serviço EC2Config.
- Para AMIs do Windows Server 2016 e posterior, use o serviço EC2Launch.

Esses procedimentos também descrevem como se conectar a uma instância se você perder o par de chaves que foi usado para criar a instância. O Amazon EC2 usa uma chave pública para criptografar uma parte dos dados, como uma senha, e uma chave privada para descriptografar os dados. As chaves pública e privada são conhecidas como par de chaves. Com instâncias Windows, você usa um par de chaves para obter a senha do administrador e faz login usando o RDP.

Note

Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte [Usar o EC2Rescue para Windows Server com o Run Command do Systems Manager](#).

Tópicos

- [Redefinir a senha de administrador do Windows usando o EC2Launch v2 \(p. 1591\)](#)
- [Redefinir a senha de administrador do Windows usando o EC2Config \(p. 1594\)](#)
- [Redefinir a senha de administrador do Windows usando o EC2Launch \(p. 1598\)](#)

Redefinir a senha de administrador do Windows usando o EC2Launch v2

Se você perdeu a senha de administrador do Windows e está usando uma AMI compatível do Windows que inclua o serviço EC2Launch v2, poderá usar o EC2Launch v2 para gerar uma nova senha.

Se estiver usando uma AMI do Windows Server 2016 ou posterior que não inclua o serviço EC2Launch v2, consulte [Redefinir a senha de administrador do Windows usando o EC2Launch \(p. 1598\)](#).

Se estiver usando uma AMI do Windows Server anterior a 2016 que não inclua o serviço EC2Launch v2, consulte [Redefinir a senha de administrador do Windows usando o EC2Config \(p. 1594\)](#).

Note

Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte [Usar o EC2Rescue para Windows Server com o Run Command do Systems Manager](#).

Note

Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte [Redefinir senhas e chaves SSH nas instâncias do Amazon EC2](#) no Guia do usuário do AWS Systems Manager.

Para redefinir a senha de administrador do Windows usando o EC2Launch v2, é necessário fazer o seguinte:

- [Etapa 1: Verificar se o serviço EC2Launch v2 está em execução \(p. 1591\)](#)
- [Etapa 2: Desanexar o volume raiz da instância \(p. 1592\)](#)
- [Etapa 3: Anexar o volume a uma instância temporária \(p. 1593\)](#)
- [Etapa 4: Excluir o arquivo .run-once \(p. 1593\)](#)
- [Etapa 5: Reiniciar a instância original \(p. 1594\)](#)

Etapa 1: Verificar se o serviço EC2Launch v2 está em execução

Antes de tentar redefinir a senha de administrador, verifique se o serviço EC2Launch v2 está instalado e em execução. O serviço EC2Launch v2 será utilizado para redefinir a senha de administrador posteriormente nesta seção.

Como verificar se o serviço EC2Launch v2 está em execução

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância que precisa de redefinição da senha. Essa instância é denominada original neste procedimento.
3. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log Obter log do sistema.
4. Localize a entrada do EC2 Launch, por exemplo, Launch: EC2Launch v2 service v2.0.124 (Launch: serviço EC2Launch v2 v2.0.124). Se essa entrada for exibida, o serviço EC2Launch v2 estará em execução.

Se a saída do log do sistema estiver vazia, ou se o serviço EC2Launch v2 não estiver em execução, solucione os problemas da instância usando o serviço Instance Console Screenshot. Para obter mais informações, consulte [Solucionar problemas de uma instância não acessível \(p. 1581\)](#).

Etapa 2: Desanexar o volume raiz da instância

Não será possível usar o EC2Launch v2 para redefinir uma senha de administrador se o volume no qual a senha está armazenada estiver anexado a uma instância como o volume raiz. Você precisa desanexar o volume da instância original antes de anexá-lo a uma instância temporária como um volume secundário.

Para desanexar o volume raiz da instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer a atualização do driver e escolha Actions (Ações), Instance state (Estado da instância), Stop instance (Parar instância). Depois que o status da instância for alterado para Stopped (Parado), siga para a próxima etapa.
4. (Opcional) Se você tiver a chave privada especificada ao iniciar esta instância, continue para a próxima etapa. Caso contrário, use as etapas a seguir para substituir a instância por uma nova que você executa com um novo par de chaves.
 - a. Crie um par de chaves usando o console do Amazon EC2. Para dar ao seu novo par de chaves um nome exatamente igual ao do par de chaves perdido, primeiro exclua o par de chaves existente.
 - b. Selecione a instância a ser substituída. Anote o tipo de instância, a VPC, a sub-rede, o grupo de segurança e a função do IAM da instância.
 - c. Escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem). Digite um nome e uma descrição para a imagem e depois escolha Create image (Criar imagem). No painel de navegação, selecione AMIs. Após o status da imagem mudar para available (disponível), vá para a próxima etapa.
 - d. Selecione a imagem e escolha Actions (Ações) e, em seguida, Launch (Iniciar).
 - e. Conclua o assistente, selecionando o mesmo tipo de instância, VPC, sub-rede, grupo de segurança e função do IAM da instância a ser substituída e escolha Launch (Iniciar).
 - f. Quando solicitado, escolha o par de chaves que você criou para a nova instância, selecione a caixa de confirmação e, então, escolha Launch Instances (Executar instâncias).
 - g. (Opcional) Se a instância original tiver um endereço IP elástico associado, transfira-o para a nova instância. Se a instância original tiver volumes do EBS além do volume raiz, transfira-os para a nova instância.
 - h. Encerre a instância interrompida, pois ela não é mais necessária. Para o restante deste procedimento, todas as referências à instância original se aplicam à instância que você acabou de criar.
5. Desanexe o volume raiz da instância original da seguinte forma:
 - a. No painel Description (Descrição) da instância original, observe o ID do volume do EBS listado como o Root device (Dispositivo raiz).

- b. No painel de navegação, escolha Volumes.
- c. Na lista de volumes, selecione o volume anotado na etapa anterior e selecione Actions (Ações) e Detach Volume (Desanexar volume). Após o status do volume mudar para available (disponível), vá para a próxima etapa.

Etapa 3: Anexar o volume a uma instância temporária

Em seguida, execute uma instância temporária e anexe o volume a ela como um volume secundário. Esta é a instância usada para modificar o arquivo de configuração.

Para executar uma instância temporária e anexar o volume

1. Inicie a instância temporária da seguinte forma:

- a. No painel de navegação, escolha Instances (Instâncias), Launch instances (Iniciar instâncias) e, em seguida, selecione uma AMI.

Important

Para evitar colisões de assinatura de disco, você deve selecionar uma AMI para uma versão diferente do Windows. Por exemplo, se a instância original executar o Windows Server 2019, inicie a instância temporária usando a AMI básica do Windows Server 2016.

- b. Selecione um tipo de instância padrão e, a seguir, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).
- c. Na página Configure Instance Details (Configurar os detalhes da instância), em Subnet (Sub-rede), selecione a mesma zona de disponibilidade que a instância original e escolha Review and Launch (Revisar e iniciar).

Important

A instância temporária deve estar na mesma zona de disponibilidade que a instância original. Se sua instância temporária estiver em uma zona de disponibilidade diferente, você não poderá anexar o volume raiz da instância original a ela.

- d. Na página Review Instance Launch, escolha Launch.
- e. Quando solicitado, crie um par de chaves, faça download para um local seguro no computador e escolha Launch Instances (Iniciar instâncias).
2. Anexe o volume à instância temporária como um volume secundário da seguinte forma:
 - a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância original e escolha Actions (Ações), Attach Volume (Anexar volume).
 - b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância temporária e selecione-a na lista.
 - c. Em Device (Dispositivo), digite **xvdf** (se já não estiver lá) e escolha Attach (Anexar).

Etapa 4: Excluir o arquivo .run-once

Depois de anexar o volume à instância temporária como um volume secundário, exclua o arquivo **.run-once** da instância, localizado em %ProgramData%/Amazon/EC2Launch/state/.run-once. Isso instrui o EC2Launch v2 a executar todas as tarefas com uma frequência de once, o que inclui a definição da senha de administrador.

Important

Todos os scripts definidos para uma execução serão acionados por essa ação.

Etapa 5: Reiniciar a instância original

Depois de excluir o arquivo `.run-once`, anexe novamente o volume à instância original como o volume raiz e conecte-se à instância usando seu par de chaves para recuperar a senha do administrador.

1. Reanexe o volume à instância original da seguinte forma:
 - a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância temporária e escolha Actions (Ações), Attach Volume (Anexar volume).
 - b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância original e selecione-a.
 - c. Em Device (Dispositivo), digite `/dev/sda1`.
 - d. Escolha Associar. Após o status do volume mudar para `in-use`, vá para a próxima etapa.
2. No painel de navegação, escolha Instances (Instâncias). Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após o estado da instância mudar para `Running`, vá para a próxima etapa.
3. Recupere a nova senha de administrador do Windows usando a chave privada do novo par de chaves e conecte-se à instância. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).

Important

A instância recebe um novo endereço IP público depois de você a interrompe e a inicia.
Não deixe de se conectar à instância usando o nome DNS público atual. Para obter mais informações, consulte [Ciclo de vida da instância \(p. 412\)](#).

4. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Redefinir a senha de administrador do Windows usando o EC2Config

Se você perdeu a senha de administrador do Windows e está usando uma AMI do Windows anterior ao Windows Server 2016, poderá usar o serviço EC2Config para gerar uma nova senha.

Se você estiver usando uma AMI do Windows Server 2016 ou posterior, consulte [Redefinir a senha de administrador do Windows usando o EC2Launch \(p. 1598\)](#).

Note

Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte [Usar o EC2Rescue para Windows Server com o Run Command do Systems Manager](#).

Note

Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte [Redefinir senhas e chaves SSH nas instâncias do Amazon EC2](#) no Guia do usuário do AWS Systems Manager.

Para redefinir sua senha de administrador do Windows usando o EC2Config, você precisa fazer o seguinte:

- [Etapa 1: Verificar se o serviço do EC2Config está em execução \(p. 1595\)](#)

- Etapa 2: Desanexar o volume raiz da instância (p. 1595)
- Etapa 3: Anexar o volume a uma instância temporária (p. 1596)
- Etapa 4: Modificar o arquivo de configuração (p. 1597)
- Etapa 5: Reiniciar a instância original (p. 1598)

Etapa 1: Verificar se o serviço do EC2Config está em execução

Antes de tentar redefinir a senha de administrador, verifique se o serviço EC2Config está instalado e em execução. Você utilizará o serviço EC2Config para redefinir a senha de administrador posteriormente nesta seção.

Para verificar se o serviço do EC2Config está em execução

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias) e selecione a instância que precisa de redefinição da senha. Essa instância é denominada original neste procedimento.
3. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema).
4. Encontre a entrada agente do EC2, por exemplo, EC2 Agent: Ec2Config service v3.18.1118 (Agente do EC2: serviço Ec2Config v3.18.1118). Se você vir essa entrada, o serviço EC2Config estará em execução.

Se a saída do log do sistema estiver vazia, ou se o serviço EC2Config não estiver em execução, solucione os problemas da instância usando o serviço Instance Console Screenshot. Para obter mais informações, consulte [Solucionar problemas de uma instância não acessível \(p. 1581\)](#).

Etapa 2: Desanexar o volume raiz da instância

Você não poderá usar o EC2Config para redefinir uma senha de administrador se o volume no qual a senha está armazenada estiver anexado a uma instância como o volume raiz. Você precisa desanexar o volume da instância original antes de anexá-lo a uma instância temporária como um volume secundário.

Para desanexar o volume raiz da instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer uma redefinição de senha e escolha Actions (Ações), Instance state (Estado da instância), Stop instance (Parar instância). Depois que o status da instância for alterado para Stopped (Parado), siga para a próxima etapa.
4. (Opcional) Se você tiver a chave privada especificada ao iniciar esta instância, continue para a próxima etapa. Caso contrário, use as etapas a seguir para substituir a instância por uma nova que você executa com um novo par de chaves.
 - a. Crie um par de chaves usando o console do Amazon EC2. Para dar ao seu novo par de chaves um nome exatamente igual ao do par de chaves perdido, primeiro exclua o par de chaves existente.
 - b. Selecione a instância a ser substituída. Anote o tipo de instância, a VPC, a sub-rede, o grupo de segurança e a função do IAM da instância.
 - c. Escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem). Digite um nome e uma descrição para a imagem e depois escolha Create image (Criar imagem). No painel de navegação, selecione AMIs. Após o status da imagem mudar para available (disponível), vá para a próxima etapa.
 - d. Selecione a imagem e escolha Actions (Ações) e, em seguida, Launch (Iniciar).

- e. Conclua o assistente, selecionando o mesmo tipo de instância, VPC, sub-rede, grupo de segurança e função do IAM da instância a ser substituída e escolha Launch (Iniciar).
 - f. Quando solicitado, escolha o par de chaves que você criou para a nova instância, selecione a caixa de confirmação e, então, escolha Launch Instances (Executar instâncias).
 - g. (Opcional) Se a instância original tiver um endereço IP elástico associado, transfira-o para a nova instância. Se a instância original tiver volumes do EBS além do volume raiz, transfira-os para a nova instância.
 - h. Encerre a instância interrompida, pois ela não é mais necessária. Para o restante deste procedimento, todas as referências à instância original se aplicam à instância que você acabou de criar.
5. Desanexe o volume raiz da instância original da seguinte forma:
 - a. No painel Description (Descrição) da instância original, observe o ID do volume do EBS listado como o Root device (Dispositivo raiz).
 - b. No painel de navegação, escolha Volumes.
 - c. Na lista de volumes, selecione o volume anotado na etapa anterior e selecione Actions (Ações) e Detach Volume (Desanexar volume). Após o status do volume mudar para available (disponível), vá para a próxima etapa.

Etapa 3: Anexar o volume a uma instância temporária

Em seguida, execute uma instância temporária e anexe o volume a ela como um volume secundário. Esta é a instância usada para modificar o arquivo de configuração.

Para executar uma instância temporária e anexar o volume

1. Inicie a instância temporária da seguinte forma:

- a. No painel de navegação, escolha Instances (Instâncias), Launch instances (Iniciar instâncias) e, em seguida, selecione uma AMI.

Important

Para evitar colisões de assinatura de disco, você deve selecionar uma AMI para uma versão diferente do Windows. Por exemplo, se a instância original executar o Windows Server 2019, inicie a instância temporária usando a AMI básica do Windows Server 2016.

- b. Selecione um tipo de instância padrão e, a seguir, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).
 - c. Na página Configure Instance Details (Configurar os detalhes da instância), em Subnet (Sub-rede), selecione a mesma zona de disponibilidade que a instância original e escolha Review and Launch (Revisar e iniciar).

Important

A instância temporária deve estar na mesma zona de disponibilidade que a instância original. Se sua instância temporária estiver em uma zona de disponibilidade diferente, você não poderá anexar o volume raiz da instância original a ela.

- d. Na página Review Instance Launch, escolha Launch.
 - e. Quando solicitado, crie um par de chaves, faça download para um local seguro no computador e escolha Launch Instances (Iniciar instâncias).
2. Anexe o volume à instância temporária como um volume secundário da seguinte forma:
 - a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância original e escolha Actions (Ações), Attach Volume (Anexar volume).

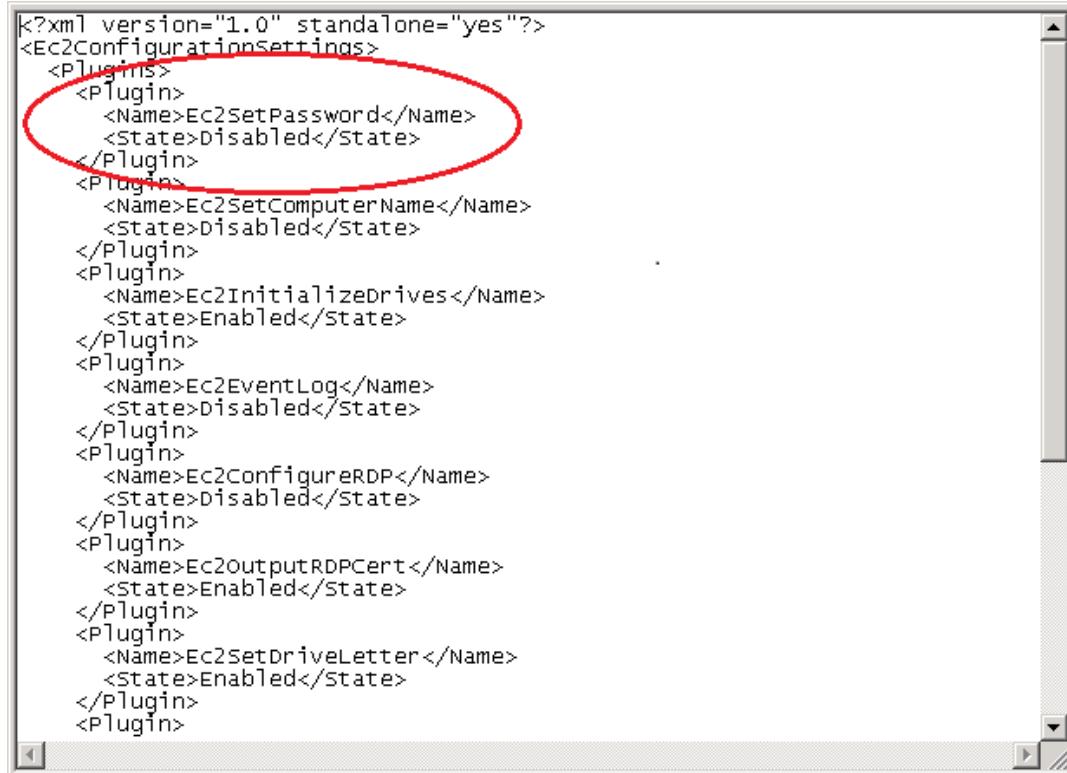
- b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância temporária e selecione-a na lista.
- c. Em Device (Dispositivo), digite **xvdf** (se já não estiver lá) e escolha Attach (Anexar).

Etapa 4: Modificar o arquivo de configuração

Depois de anexar o volume à instância temporária como um volume secundário, modifique o plug-in Ec2SetPassword no arquivo de configuração.

Para modificar o arquivo de configuração

1. Na instância temporária, modifique o arquivo de configuração no volume secundário da seguinte maneira:
 - a. Execute a instância temporária e conecte-se a ela.
 - b. Abra o utilitário Disk Management (Gerenciamento de disco) e ative a unidade online seguindo estas instruções: [Disponibilização de um volume do Amazon EBS para uso](#).
 - c. Navegue até o volume secundário e abra \Program Files\Amazon\Ec2ConfigService\Settings\config.xml usando um editor de texto, como o Bloco de notas.
 - d. Na parte superior do arquivo, localize o plugin com o nome Ec2SetPassword, como mostrado no screenshot. Altere o estado de Disabled para Enabled e salve o arquivo.



```
<?xml version="1.0" standalone="yes"?>
<Ec2ConfigurationSettings>
  <Plugins>
    <Plugin>
      <Name>Ec2SetPassword</Name>
      <State>Disabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2SetComputerName</Name>
      <State>Disabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2InitializeDrives</Name>
      <State>Enabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2EventLog</Name>
      <State>Disabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2ConfigureRDP</Name>
      <State>Disabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2OutputRDPCert</Name>
      <State>Enabled</State>
    </Plugin>
    <Plugin>
      <Name>Ec2SetDriveLetter</Name>
      <State>Enabled</State>
    </Plugin>
  </Plugins>
</Ec2ConfigurationSettings>
```

2. Depois de modificar o arquivo de configuração, desconecte o volume secundário da instância temporária da seguinte maneira:
 - a. Usando o utilitário Disk Management (Gerenciamento de disco), desative o volume.
 - b. Desconecte-se da instância temporária e volte para o console Amazon EC2.

- c. No painel de navegação, selecione Volumes, selecione o volume e escolha Actions (Ações), Detach Volume (Desanexar volume). Quando o status do volume mudar para available (disponível), vá para a próxima etapa.

Etapa 5: Reiniciar a instância original

Depois de modificar o arquivo de configuração, reconecte o volume à instância original como o volume raiz e conecte-se à instância usando seu par de chaves para recuperar a senha do administrador.

1. Reanexe o volume à instância original da seguinte forma:
 - a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância temporária e escolha Actions (Ações), Attach Volume (Anexar volume).
 - b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância original e selecione-a.
 - c. Em Device (Dispositivo), digite **/dev/sda1**.
 - d. Escolha Associar. Após o status do volume mudar para in-use, vá para a próxima etapa.
2. No painel de navegação, escolha Instances (Instâncias). Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após o estado da instância mudar para Running, vá para a próxima etapa.
3. Recupere a nova senha de administrador do Windows usando a chave privada do novo par de chaves e conecte-se à instância. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).

Important

A instância recebe um novo endereço IP público depois de você a interrompe e a inicia. Não deixe de se conectar à instância usando o nome DNS público atual. Para obter mais informações, consulte [Ciclo de vida da instância \(p. 412\)](#).

4. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Redefinir a senha de administrador do Windows usando o EC2Launch

Se você esqueceu a senha de administrador do Windows e está usando uma AMI do Windows Server 2016 ou posterior, poderá usar a ferramenta EC2Rescue que utiliza o serviço EC2Launch para gerar uma nova senha.

Se você estiver usando uma AMI do Windows Server anterior ao Windows Server 2016, consulte [Redefinir a senha de administrador do Windows usando o EC2Config \(p. 1594\)](#).

Warning

Quando você interrompe uma instância, os dados em todos os volumes de armazenamento de instâncias são apagados. Para manter dados longe dos volumes de armazenamento de instância, faça backup no armazenamento persistente.

Note

Se você desabilitou a conta de administrador local na instância e sua instância estiver configurada para o Systems Manager, você também poderá reabilitar e redefinir sua senha de administrador local usando EC2Rescue e o Run Command. Para obter mais informações, consulte [Usar o EC2Rescue para Windows Server com o Run Command do Systems Manager](#).

Note

Existe um documento de automação do AWS Systems Manager que aplica automaticamente as etapas manuais necessárias para redefinir a senha do administrador local. Para obter mais informações, consulte [Redefinir senhas e chaves SSH nas instâncias do Amazon EC2](#) no Guia do usuário do AWS Systems Manager.

Para redefinir sua senha de administrador do Windows usando o EC2Launch, você precisa fazer o seguinte:

- [Etapa 1: Desanexar o volume raiz da instância \(p. 1599\)](#)
- [Etapa 2: Anexar o volume a uma instância temporária \(p. 1600\)](#)
- [Etapa 3: Redefinir a senha de administrador \(p. 1600\)](#)
- [Etapa 4: Reiniciar a instância original \(p. 1601\)](#)

Etapa 1: Desanexar o volume raiz da instância

Você não poderá usar o EC2Launch para redefinir uma senha de administrador se o volume no qual a senha está armazenada estiver anexado a uma instância como o volume raiz. Você precisa desanexar o volume da instância original antes de anexá-lo a uma instância temporária como um volume secundário.

Para desanexar o volume raiz da instância

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância que requer uma redefinição de senha e escolha Actions (Ações), Instance state (Estado da instância), Stop instance (Parar instância). Depois que o status da instância for alterado para Stopped (Parado), siga para a próxima etapa.
4. (Opcional) Se você tiver a chave privada especificada ao iniciar esta instância, continue para a próxima etapa. Caso contrário, use as etapas a seguir para substituir a instância por uma nova que você executa com um novo par de chaves.
 - a. Crie um par de chaves usando o console do Amazon EC2. Para dar ao seu novo par de chaves um nome exatamente igual ao do par de chaves perdido, primeiro exclua o par de chaves existente.
 - b. Selecione a instância a ser substituída. Anote o tipo de instância, a VPC, a sub-rede, o grupo de segurança e a função do IAM da instância.
 - c. Escolha Actions (Ações), Image and templates (Imagem e modelos), Create image (Criar imagem). Digite um nome e uma descrição para a imagem e depois escolha Create image (Criar imagem). No painel de navegação, selecione AMIs. Após o status da imagem mudar para available (disponível), vá para a próxima etapa.
 - d. Selecione a imagem e escolha Actions (Ações) e, em seguida, Launch (Iniciar).
 - e. Conclua o assistente, selecionando o mesmo tipo de instância, VPC, sub-rede, grupo de segurança e função do IAM da instância a ser substituída e escolha Launch (Iniciar).
 - f. Quando solicitado, escolha o par de chaves que você criou para a nova instância, selecione a caixa de confirmação e, então, escolha Launch Instances (Executar instâncias).
 - g. (Opcional) Se a instância original tiver um endereço IP elástico associado, transfira-o para a nova instância. Se a instância original tiver volumes do EBS além do volume raiz, transfira-os para a nova instância.
 - h. Encerre a instância interrompida, pois ela não é mais necessária. Para o restante deste procedimento, todas as referências à instância original se aplicam à instância que você acabou de criar.
5. Desanexe o volume raiz da instância original da seguinte forma:

- a. No painel Description (Descrição) da instância original, observe o ID do volume do EBS listado como o Root device (Dispositivo raiz).
- b. No painel de navegação, escolha Volumes.
- c. Na lista de volumes, selecione o volume anotado na etapa anterior e selecione Actions (Ações) e Detach Volume (Desanexar volume). Após o status do volume mudar para available (disponível), vá para a próxima etapa.

Etapa 2: Anexar o volume a uma instância temporária

Em seguida, execute uma instância temporária e anexe o volume a ela como um volume secundário. Esta é a instância que você usa para executar o EC2Launch.

Para executar uma instância temporária e anexar o volume

1. Inicie a instância temporária da seguinte forma:

- a. No painel de navegação, escolha Instances (Instâncias), Launch instances (Iniciar instâncias) e, em seguida, selecione uma AMI.

Important

Para evitar colisões de assinatura de disco, você deve selecionar uma AMI para uma versão diferente do Windows. Por exemplo, se a instância original executar o Windows Server 2019, inicie a instância temporária usando a AMI básica do Windows Server 2016.

- b. Selecione um tipo de instância padrão e, a seguir, escolha Next: Configure Instance Details (Próximo: Configurar detalhes da instância).
 - c. Na página Configure Instance Details (Configurar os detalhes da instância), em Subnet (Sub-rede), selecione a mesma zona de disponibilidade que a instância original e escolha Review and Launch (Revisar e iniciar).

Important

A instância temporária deve estar na mesma zona de disponibilidade que a instância original. Se sua instância temporária estiver em uma zona de disponibilidade diferente, você não poderá anexar o volume raiz da instância original a ela.

- d. Na página Review Instance Launch, escolha Launch.
 - e. Quando solicitado, crie um par de chaves, faça download para um local seguro no computador e escolha Launch Instances (Iniciar instâncias).
2. Anexe o volume à instância temporária como um volume secundário da seguinte forma:
 - a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância original e escolha Actions (Ações), Attach Volume (Anexar volume).
 - b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância temporária e selecione-a na lista.
 - c. Em Device (Dispositivo), digite **xvdf** (se já não estiver lá) e escolha Attach (Anexar).

Etapa 3: Redefinir a senha de administrador

Em seguida, conecte-se à instância temporária e use o EC2Launch para redefinir a senha do administrador.

Para redefinir a senha de administrador

1. Conecte-se à instância temporária e use a ferramenta EC2Rescue for Windows Server na instância para redefinir a senha de administrador, da seguinte maneira:
 - a. Faça download do arquivo zip [EC2Rescue for Windows Server](#), extraia o conteúdo e execute EC2Rescue.exe.
 - b. Na tela License Agreement (Contrato de licença), leia o contrato de licença e, se você aceitar os termos, escolha I Agree (Eu aceito).
 - c. Na tela Welcome to EC2Rescue for Windows Server (Bem-vindo ao EC2Rescue for Windows Server), escolha Next (Avançar).
 - d. Na tela Select mode (Selecionar modo), escolha Offline instance (Instância offline).
 - e. Na tela Select a disk (Selecionar um disco), selecione o dispositivo xvdf e, em seguida, Next (Avançar).
 - f. Confirme a seleção do disco e escolha Yes.
 - g. Depois que o volume for carregado, escolha OK.
 - h. Na tela Select Offline Instance Option (Selecionar opção de instância offline), escolha Diagnose and Rescue (Diagnosticar e recuperar).
 - i. Na tela Summary (Resumo), leia as informações e escolha Next (Avançar).
 - j. Na tela Detected possible issues (Problemas possíveis detectados), selecione Reset Administrator Password (Redefinir senha do administrador) e escolha Next (Avançar).
 - k. Na tela Confirm (Confirmar), escolha Rescue (Recuperar), OK.
 - l. Na tela Done (Concluído), escolha Finish (Concluir).
 - m. Feche a ferramenta EC2Rescue for Windows Server, desconecte-se da instância temporária e, em seguida, retorne para o console do Amazon EC2.
2. Desanexe o volume (xvdf) secundário da instância temporária da seguinte forma:
 - a. No painel de navegação, escolha Instances (Instâncias) e selecione a instância temporária.
 - b. Na guia Storage (Armazenamento) da instância temporária, observe o ID do volume do EBS listado como xvdf.
 - c. No painel de navegação, escolha Volumes.
 - d. Na lista de volumes, selecione o volume anotado na etapa anterior e selecione Actions (Ações) e Detach Volume (Desanexar volume). Após o status do volume mudar para available (disponível), vá para a próxima etapa.

Etapa 4: Reiniciar a instância original

Depois de redefinir a senha do administrador usando o EC2Launch, reconecte o volume à instância original como o volume raiz e conecte-se à instância usando seu par de chaves para recuperar a senha do administrador.

Para reiniciar a instância original

1. Reanexe o volume à instância original da seguinte forma:
 - a. No painel de navegação, selecione Volumes, selecione o volume que você desanexou da instância temporária e escolha Actions (Ações), Attach Volume (Anexar volume).
 - b. Na caixa de diálogo Attach Volume (Anexar volume), em Instances (Instâncias), comece a digitar o nome ou ID da instância original e selecione-a.
 - c. Em Device (Dispositivo), digite **/dev/sda1**.
 - d. Escolha Associar. Após o status do volume mudar para **in-use**, vá para a próxima etapa.

2. No painel de navegação, escolha Instances (Instâncias). Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após o estado da instância mudar para Running, vá para a próxima etapa.
3. Recupere a nova senha de administrador do Windows usando a chave privada do novo par de chaves e conecte-se à instância. Para obter mais informações, consulte [Conectar-se à sua instância do Windows \(p. 443\)](#).
4. (Opcional) Você pode encerrar a instância temporária se não tiver utilização adicional para ela. Selecione a instância temporária e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).

Solução de problemas na interrupção da instância

Se você tiver parado sua instância com Amazon EBS e parecer que ela travou no estado `stopping`, pode haver um problema com o computador host subjacente.

Não existe qualquer custo para uso da instância enquanto ela está no estado `stopping` ou em qualquer outro estado, exceto `running`. Você só é cobrado pelo uso da instância quando ela está no estado `running`.

Forçar a parada da instância

Force a interrupção da instância usando o console ou a AWS CLI.

New console

Para forçar a parada da instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instances (Instâncias) e selecione a instância travada.
3. Escolha Instance state (Estado da instância), Force stop instance (Forçar parada da parada), Stop (Parar).

Old console

Para forçar a parada da instância usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instances (Instâncias) e selecione a instância travada.
3. Escolha Instance State (Estado da instância), Stop (Parar), Yes, Forcefully Stop (Sim, parar à força).

AWS CLI

Para forçar a parada da instância usando a AWS CLI

Use o comando `stop-instances` e a opção `--force` da seguinte forma:

```
aws ec2 stop-instances --instance-ids i-0123ab456c789d01e --force
```

Se, após 10 minutos, a instância não foi interrompida, publique uma solicitação de ajuda no [fórum do Amazon EC2](#). Para ajudar a agilizar uma resolução, inclua o ID da instância e descreva as etapas que

você já realizou. Alternativamente, se você possui um plano de suporte, crie um caso de suporte técnico no [Atendimento ao cliente](#).

Para criar uma instância de substituição

Para tentar resolver o problema enquanto você espera pela assistência do [fórum do Amazon EC2](#) ou da [Central de Suporte](#), crie uma instância de substituição. Crie uma AMI da instância travada e execute uma nova instância usando a nova AMI.

New console

Para criar uma instância de substituição usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instances (Instâncias) e selecione a instância travada.
3. Escolha Actions (Ações), Image and templates (Imagen e modelos), Create image (Criar imagem).
4. Na página Create image (Criar imagem), faça o seguinte:
 - a. Digite um nome e uma descrição para a AMI.
 - b. Escolha Sem reinicialização.
 - c. Escolha Create Image (Criar imagem).

Para obter mais informações, consulte [Criar uma AMI do Windows em uma instância em execução \(p. 40\)](#).

5. Execute uma nova instância a partir da AMI e verifique se a instância nova está funcionando.
6. Selecione a instância travada e escolha Actions (Ações), Instance state (Estado da instância) e Terminate (Encerrar). Se a instância também ficar travada ao ser encerrada, o Amazon EC2 automaticamente forçará o encerramento dela dali a algumas horas.

Old console

Para criar uma instância de substituição usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instances (Instâncias) e selecione a instância travada.
3. Escolha Ações, Imagem, Criar imagem.
4. Na caixa de diálogo Create Image (Criar imagem), preencha os campos a seguir e, em seguida, escolha Create Image:
 - a. Especifique um nome e uma descrição da AMI.
 - b. Escolha Sem reinicialização.

Para obter mais informações, consulte [Criar uma AMI do Windows em uma instância em execução \(p. 40\)](#).

5. Execute uma nova instância a partir da AMI e verifique se a instância nova está funcionando.
6. Selecione a instância travada e escolha Actions (Ações), depois Instance State (Estado da instância) e Terminate (Encerrar). Se a instância também ficar travada ao ser encerrada, o Amazon EC2 automaticamente forçará o encerramento dela dali a algumas horas.

AWS CLI

Para criar uma instância de substituição usando a CLI

1. Crie uma AMI da instância travada usando o comando [create-image](#) (AWS CLI) e a opção `--no-reboot` da seguinte forma:

```
aws ec2 create-image --instance-id i-0123ab456c789d01e --name "AMI" --  
description "AMI for replacement instance" --no-reboot
```

2. Execute uma nova instância da AMI usando o comando [run-instances](#) (AWS CLI) da seguinte forma:

```
aws ec2 run-instances --image-id ami-1a2b3c4d --count 1 --instance-type c3.large --  
key-name MyKeyPair --security-groups MySecurityGroup
```

3. Verifique se a nova instância está funcionando.
4. Encerre a instância travada usando o comando [terminate-instances](#) (AWS CLI) da seguinte forma:

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

Caso você não consiga criar uma AMI a partir da instância, conforme descrito no procedimento anterior, configure uma instância de substituição da seguinte forma:

(Alternativa) Para criar uma instância de substituição usando o console

1. Selecione a instância e escolha Description (Descrição), Block devices (Dispositivos de bloco). Selecione cada volume e anote o ID do volume. Note qual é o volume do dispositivo raiz.
2. No painel de navegação, escolha Volumes. Selecione cada volume para a instância e escolha Ações, Criar snapshot.
3. No painel de navegação, selecione Snapshots. Selecione o snapshot que você acabou de criar, e escolha Ações, Criar volume.
4. Execute uma instância com o mesmo sistema operacional da instância travada. Observe o ID do volume e o nome do dispositivo de seu volume do dispositivo raiz.
5. No painel de navegação, escolha Instances (Instâncias), selecione a instância que acabou de executar e escolha Instance state (Estado da instância) e Stop instance (Parar instância).
6. No painel de navegação, selecione Volumes, selecione o volume do dispositivo raiz da instância parada e escolha Ações, Separar volume.
7. Selecione o volume do dispositivo raiz de que você criou usando a instância presa, selecione Actions (Actions), Attach Volume (Associar volume) e associe-o à nova instância como volume raiz (usando o nome do dispositivo que você anotou). Associe todos os volumes adicionais não raiz à instância.
8. No painel de navegação, selecione Instâncias e selecione a instância de substituição. Escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Verifique se a instância está trabalhando.
9. Selecione a instância travada e escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância). Se a instância também ficar travada ao ser encerrada, o Amazon EC2 automaticamente fará o encerramento dela daqui a algumas horas.

Solucionar problemas de encerramento (desativação) da instância

Você não paga por nenhum uso de instância enquanto ela não estiver no estado `running`. Em outras palavras, ao encerrar uma instância, você para de ser cobrado por ela assim que o estado mudar para `shutting-down`.

A instância é encerrada imediatamente

Vários problemas podem fazer com que a sua instância seja encerrada imediatamente na inicialização. Consulte [A instância é encerrada imediatamente \(p. 1572\)](#) para obter mais informações.

Encerramento atrasado da instância

Se sua instância permanecer no estado `shutting-down` por mais do que alguns minutos, ela poderá ser atrasada porque os scripts de desativação estão sendo executados pela instância.

Outra causa possível é um problema com o computador host subjacente. Se sua instância permanecer no estado `shutting-down` por várias horas, o Amazon EC2 a tratará como uma instância travada e a encerrará à força.

Se parecer que sua instância está travada no encerramento e tiverem se passado várias horas, publique uma solicitação de ajuda no [fórum do Amazon EC2](#). Para ajudar a agilizar uma resolução, inclua o ID da instância e descreva as etapas que já tomou. Alternativamente, se você possui um plano de suporte, crie um caso de suporte técnico no [Atendimento ao cliente](#).

Instância encerrada ainda sendo exibida

Depois de encerrar uma instância, ela permanecerá visível por um breve período antes de ser excluída. O estado mostra `terminated`. Se a entrada não for excluída depois de várias horas, entre em contato com o Suporte.

Instâncias executadas ou encerradas automaticamente

De modo geral, os comportamentos a seguir indicam que você usou o Amazon EC2 Auto Scaling, a frota do EC2 ou a frota spot para escalar os recursos de computação automaticamente com base nos critérios que você definiu.

- Você encerra uma instância e uma nova instância é iniciada automaticamente.
- Você inicia uma instância e uma de suas instâncias é encerrada automaticamente.
- Você interrompe uma instância e ela é encerrada e uma nova instância é iniciada automaticamente.

Para interromper a escalabilidade automática, consulte o [Guia do usuário do Amazon EC2 Auto Scaling, EC2 Fleet \(p. 712\)](#) ou [Criar uma solicitação de frota spot \(p. 776\)](#).

Solucionar problemas do Sysprep

Se você tiver problemas ou receber mensagens de erro durante as preparações da imagem, veja os logs a seguir. A localização do log depende do que você está executando, EC2Config ou EC2Launch com Sysprep.

- %WINDIR%\Panther\Unattendgc (EC2Config e EC2Launch)
- %WINDIR%\System32\Sysprep\Panther (EC2Config e EC2Launch)
- C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt (somente EC2Config)
- C:\ProgramData\Amazon\Ec2Config\Logs (somente EC2Config)
- C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log (somente EC2Launch)

Se você receber uma mensagem de erro durante a preparação de imagem com Sysprep, o SO poderá não ser alcançável. Para analisar os arquivos de log, é preciso primeiro parar a instância, associar o volume do dispositivo raiz a outra instância íntegra como volume secundário e analisar os logs mencionados anteriormente no volume secundário. Para obter mais informações sobre a finalidade dos arquivos de log por nome, consulte [Arquivos de log relacionados à configuração do Windows](#) na documentação da Microsoft.

Se você encontrar erros no arquivo de log Unattendgc, use a [Ferramenta de pesquisa de erro da Microsoft](#) para obter mais detalhes sobre o erro. O problema a seguir relatado no arquivo Unattendgc é geralmente o resultado de um ou mais perfis de usuário corrompidos na instância:

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Há duas opções para resolver o problema:

Opção 1: use o Regedit na instância para pesquisar pela chave a seguir. Verifique se não há chaves do registro de perfil para um usuário excluído:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\]
```

Opção 2: edite o arquivo de resposta EC2Config (C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml) e altere <CopyProfile>true</CopyProfile> para <CopyProfile>false</CopyProfile>. Execute novamente o Sysprep. Observe que essa mudança de configuração excluirá o perfil de usuário do administrador incorporado após o Sysprep concluir.

Usar o EC2Rescue for Windows Server

O EC2Rescue for Windows Server é uma ferramenta fácil de usar que você executa em uma instância do Windows Server do Amazon EC2 para diagnosticar e solucionar os possíveis problemas. A ferramenta é valiosa para coletar arquivos de log e solucionar problemas e também para pesquisar proativamente possíveis áreas de preocupação. Ele pode até examinar volumes raiz do Amazon EBS de outras instâncias e coletar logs relevantes para solucionar problemas de instâncias do Windows Server que usam esse volume.

A ferramenta EC2Rescue for Windows Server tem dois módulos diferentes: um módulo coletor de dados que coleta dados de todas as diferentes origens, e um módulo analisador que analisa os dados coletados em relação a uma série de regras predefinidas para identificar problemas e fornecer sugestões.

A ferramenta EC2Rescue for Windows Server é executada apenas em instâncias do Amazon EC2 que executam o Windows Server 2008 R2 e posterior. Quando a ferramenta é iniciada, ela verifica se está sendo executada em uma instância do Amazon EC2.

O runbook [AWSSupport-ExecuteEC2Rescue](#) usa a ferramenta EC2Rescue para solucionar problemas e, quando possível, reparar problemas comuns de conectividade com a instância do EC2 especificada. Para obter mais informações e para executar essa automação, consulte [AWSSupport-ExecuteEC2Rescue](#).

Note

Se você estiver usando uma instância Linux, consulte [EC2Rescue para Linux](#).

Contents

- [Usar a GUI EC2Rescue for Windows Server \(p. 1607\)](#)
- [Usar o EC2Rescue for Windows Server com a linha de comando \(p. 1611\)](#)
- [Usar o EC2Rescue for Windows Server com o Run Command do Systems Manager \(p. 1616\)](#)

Usar a GUI EC2Rescue for Windows Server

O EC2Rescue for Windows Server pode executar as seguintes análises em instâncias offline :

Opção	Descrição
Diagnóstico e resgate	<p>O EC2Rescue for Windows Server pode detectar e resolver problemas com as seguintes configurações de serviço:</p> <ul style="list-style-type: none">• Hora do sistema<ul style="list-style-type: none">• RealTimeisUniversal: detecta se a chave do registro <code>RealTimeisUniversal</code> está habilitada. Se estiver desabilitada, a hora do sistema Windows derivará quando o fuso horário estiver definido como um valor diferente de UTC.• Firewall do Windows<ul style="list-style-type: none">• Domain networks (Redes de domínio): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.• Private networks (Redes privadas): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.• Guest or public networks (Redes públicas ou de convidado): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.• Desktop remoto<ul style="list-style-type: none">• Service Start (Início do serviço): detecta se o serviço Área de Trabalho Remota está habilitado.• Remote Desktop Connections (Conexões da Área de Trabalho Remota): detecta se essa opção está habilitada.• TCP Port (Porta TCP): detecta a porta em que o serviço Área de Trabalho Remota está ouvindo.• EC2Config (Windows Server 2012 R2 e anteriores)<ul style="list-style-type: none">• Installation (Instalação): detecta qual versão do EC2Config está instalada.

Opção	Descrição
	<ul style="list-style-type: none"> • Service Start (Início do serviço): detecta se o serviço EC2Config está habilitado. • Ec2SetPassword: gera uma nova senha de administrador. • Ec2HandleUserData: permite que você execute um script de dados de usuário na próxima inicialização da instância. • EC2Launch (Windows Server 2016 e posterior) <ul style="list-style-type: none"> • Installation (Instalação): detecta qual versão do EC2Launch está instalada. • Ec2SetPassword: gera uma nova senha de administrador. • Interface de rede <ul style="list-style-type: none"> • DHCP Service Startup (Inicialização do serviço DHCP): detecta se o serviço DHCP está habilitado. • Ethernet detail (Detalhes da Ethernet): exibe informações sobre a versão do driver de rede, se detectado. • DHCP on Ethernet (DHCP na Ethernet): detecta se o DHCP está habilitado.
Restaurar	Execute uma das seguintes ações: <ul style="list-style-type: none"> • Last Known Good Configuration (Última configuração válida conhecida): tenta inicializar a instância no estado inicializável mais recente conhecido. • Restore registry from backup (Restaurar registro do backup): restaura o registro de \Windows\System32\config\RegBack.
Capturar logs	Permite que você capture logs na instância para análise.

O EC2Rescue for Windows Server pode coletar os seguintes dados de instâncias ativas e offline:

Item	Descrição
Log de eventos	Coleta logs do aplicativo, do sistema e de eventos do EC2Config.
Registro	Coleta os hives SYSTEM e SOFTWARE.
Log do Windows Update	Coleta arquivos de log gerados pelo Windows Update.

Item	Descrição
	<p>Note</p> <p>No Windows Server 2016 e posterior, o log é coletado no formato Event Tracing for Windows (ETW, Rastreamento de Eventos para Windows).</p>
Log do Sysprep	Coleta os arquivos de log gerados pela ferramenta de Preparação do sistema Windows.
Registro de configuração da unidade	Coleta os logs da SetupAPI do Windows (<code>setupapi.dev.log</code> e <code>setupapi.setup.log</code>).
Configuração da inicialização	Coleta o hive <code>HKEY_LOCAL_MACHINE\BCD00000000</code> .
Despejo de memória	Coleta todos os arquivos de despejo de memória existentes na instância.
Arquivo do EC2Config	Coleta os arquivos de log gerados pelo serviço EC2Config.
Arquivo do EC2Launch	Coleta os arquivos de log gerados pelos scripts do EC2Launch.
Arquivo de agente do SSM	Coleta arquivos de log gerados pelo Agente SSM e pelos logs do Patch Manager.
Arquivo ElasticGPUs do EC2	Recolhe os logs de eventos relacionados a GPUs elásticas.
ECS	Coleta logs relacionados ao Amazon ECS.
CloudEndure	Coleta arquivos de log relacionados ao agente CloudEndure.

EC2Rescue for Windows Server pode coletar os seguintes dados adicionais de instâncias ativas:

Item	Descrição
Informações do sistema	Coleta MSInfo32.
Resultado da política de grupo	Coleta um relatório de políticas de grupo.

Demonstração em vídeo

Brandon mostra como usar o recurso de Diagnóstico e captura da EC2Rescue for Windows Server:

[AWS Vídeos da Central de conhecimento da : Como usar o recurso de diagnóstico e resgate do EC2Rescue?](#)

Analisar uma instância offline

A opção Offline Instance é útil para a depuração de problemas de inicialização com instâncias do Windows.

Para executar uma ação em uma instância off-line

1. Em uma instância do Windows Server em execução, faça download da ferramenta [EC2Rescue for Windows Server](#) e extraia os arquivos.

Você pode executar o seguinte comando do PowerShell para baixar o EC2Rescue sem alterar a configuração de segurança aprimorada do Internet Explorer (ESC):

```
PS C:\> Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/  
EC2Rescue_latest.zip -OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Esse comando fará download do arquivo .zip do EC2Rescue para a área de trabalho do usuário atualmente conectado.

2. Pare a instância com falha, se ela ainda não estiver parada.
3. Desanexe o volume raiz do EBS da instância com falha e anexe o volume a uma instância do Windows em funcionamento que tenha a EC2Rescue for Windows Server instalada.
4. Execute a ferramenta EC2Rescue for Windows Server na instância em funcionamento e escolha Offline Instance.
5. Selecione o disco do volume recém-montado e escolha Next.
6. Confirme a seleção do disco e escolha Yes.
7. Escolha a opção de instância off-line a ser executada e escolha Next.

A ferramenta EC2Rescue for Windows Server verifica o volume e coleta informações para solução de problemas com base nos arquivos de log selecionados.

Coletar dados de uma instância ativa

Você pode coletar logs e outros dados de uma instância ativa.

Para coletar dados de uma instância ativa

1. Conecte-se à sua instância do Windows.
2. Faça download da ferramenta [EC2Rescue for Windows Server](#) na instância do Windows e extraia os arquivos.

Você pode executar o seguinte comando do PowerShell para baixar o EC2Rescue sem alterar a configuração de segurança aprimorada do Internet Explorer (ESC):

```
PS C:\> Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/  
EC2Rescue_latest.zip -OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
```

Esse comando fará download do arquivo .zip do EC2Rescue para a área de trabalho do usuário atualmente conectado.

3. Abra o aplicativo da EC2Rescue for Windows Server e aceite o contrato de licença.
4. Escolha Next, Current instance, Capture logs.
5. Selecione os itens de dados a serem coletados e escolha Collect.... Leia o aviso e escolha Yes para continuar.
6. Escolha um nome de arquivo e um local do arquivo ZIP e escolha Save.
7. Depois que a EC2Rescue for Windows Server for concluída, escolha Open Containing Folder para visualizar o arquivo ZIP.
8. Escolha Finish.

Usar o EC2Rescue for Windows Server com a linha de comando

A interface de linha de comando (CLI) do EC2Rescue for Windows Server permite executar um plug-in do EC2Rescue for Windows Server (conhecido como “ação”) de forma programada.

O ferramenta EC2Rescue for Windows Server tem dois modos de execução:

- /online — Permite agir na instância em que o EC2Rescue for Windows Server está instalado, como coletar arquivos de log.
- /offline:<device_id>—Permite agir no volume raiz offline que está associado a uma instância separada do Amazon EC2 do Windows em que você instalou o EC2Rescue for Windows Server.

Faça download da ferramenta [EC2Rescue for Windows Server](#) na instância Windows e extraia os arquivos. É possível visualizar o arquivo de ajuda usando o seguinte comando:

```
EC2RescueCmd.exe /help
```

O EC2Rescue for Windows Server pode executar as seguintes ações na instância do Windows do Amazon EC2:

- [Ação de coleta \(p. 1611\)](#)
- [Ação de salvamento \(p. 1613\)](#)
- [Ação de restauração \(p. 1615\)](#)

Ação de coleta

Note

Você pode coletar todos os logs, um grupo inteiro de log ou um log individual dentro de um grupo.

O EC2Rescue for Windows Server pode coletar os seguintes dados de instâncias ativas e offline.

Grupo de logs	Logs disponíveis	Descrição
all		Coleta todos os logs disponíveis.
eventlog	<ul style="list-style-type: none">• 'Application'• 'System'• 'EC2ConfigService'	Coleta logs do aplicativo, do sistema e de eventos do EC2Config.
memory-dump	<ul style="list-style-type: none">• 'Memory Dump File'• 'Mini Dump Files'	Coleta todos os arquivos de despejo de memória existentes na instância.
ec2config	<ul style="list-style-type: none">• 'Log Files'• 'Configuration Files'	Coleta os arquivos de log gerados pelo serviço EC2Config.
ec2launch	<ul style="list-style-type: none">• 'Logs'• 'Config'	Coleta os arquivos de log gerados pelos scripts do EC2Launch.

Grupo de logs	Logs disponíveis	Descrição
ssm-agent	<ul style="list-style-type: none"> • 'Log Files' • 'Patch Baseline Logs' • 'InstanceData' 	Coleta arquivos de log gerados pelo Agente SSM e pelos logs do Patch Manager.
sysprep	'Log Files'	Coleta os arquivos de log gerados pela ferramenta de Preparação do sistema Windows.
driver-setup	<ul style="list-style-type: none"> • 'SetupAPI Log Files' • 'DPInst Log File' • 'AWS PV Setup Log File' 	Coleta os logs da SetupAPI do Windows (setupapi.dev.log e setupapi.setup.log).
registry	<ul style="list-style-type: none"> • 'SYSTEM' • 'SOFTWARE' • 'BCD' 	Coleta os hives SYSTEM e SOFTWARE.
egpu	<ul style="list-style-type: none"> • 'Event Log' • 'System Files' 	Recolhe os logs de eventos relacionados a GPUs elásticas.
boot-config	'BCDEDIT Output'	Coleta o hive HKEY_LOCAL_MACHINE \BCD00000000.
windows-update	'Log Files'	<p>Coleta arquivos de log gerados pelo Windows Update.</p> <p>Note</p> <p>No Windows Server 2016 e posterior, o log é coletado no formato Event Tracing for Windows (ETW, Rastreamento de Eventos para Windows).</p>
cloudendure	<ul style="list-style-type: none"> • 'Migrate Script Logs' • 'Driver Logs' • 'CloudEndure File List' 	Coleta arquivos de log relacionados ao agente CloudEndure.

O EC2Rescue for Windows Server pode coletar os seguintes dados adicionais de instâncias ativas.

Grupo de logs	Logs disponíveis	Descrição
system-info	'MSInfo32 Output'	Coleta MSInfo32.
gpresult	'GPResult Output'	Coleta um relatório de políticas de grupo.

As seguintes opções estão disponíveis:

- `/output:<outputFilePath>`: localização do caminho de arquivo de destino obrigatório para salvar arquivos de log coletados no formato zip.

- /no-offline: atributo opcional usado no modo offline. Não define o volume offline após completar a ação.
- /no-fix-signature: atributo opcional usado no modo offline. Não conserta uma possível colisão de assinatura de disco após concluir a ação.

Examples

A seguir, exemplos usando a CLI do EC2Rescue for Windows Server.

Exemplos de modo online

Coleta todos os logs disponíveis:

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Coleta somente um grupo específico de log:

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Coleta logs individuais dentro de um grupo de log:

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI Log Files' /output:<outputFilePath>
```

Exemplos de modo offline

Coleta todos os logs disponíveis de um volume do EBS. O volume é especificado pelo valor device_id.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Coleta somente um grupo específico de log:

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Ação de salvamento

O EC2Rescue for Windows Server pode detectar e resolver problemas com as seguintes configurações de serviço:

Grupo de serviço	Ações disponíveis	Descrição
all		
system-time	'RealTimeIsUniversal'	<p>Hora do sistema</p> <ul style="list-style-type: none">• RealTimeIsUniversal: detecta se a chave do registro <code>RealTimeIsUniversal</code> está habilitada. Se estiver desabilitada, a hora do sistema Windows derivará quando o fuso horário estiver definido como um valor diferente de UTC.

Grupo de serviço	Ações disponíveis	Descrição
<code>firewall</code>	<ul style="list-style-type: none"> • 'Domain networks' • 'Private networks' • 'Guest or public networks' 	Firewall do Windows <ul style="list-style-type: none"> • Domain networks (Redes de domínio): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado. • Private networks (Redes privadas): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado. • Guest or public networks (Redes públicas ou de convidado): detecta se o perfil do Firewall do Windows está habilitado ou desabilitado.
<code>rdp</code>	<ul style="list-style-type: none"> • 'Service Start' • 'Remote Desktop Connections' • 'TCP Port' 	Desktop remoto <ul style="list-style-type: none"> • Service Start (Início do serviço): detecta se o serviço Área de Trabalho Remota está habilitado. • Remote Desktop Connections (Conexões da Área de Trabalho Remota): detecta se essa opção está habilitada. • TCP Port (Porta TCP): detecta a porta em que o serviço Área de Trabalho Remota está ouvindo.
<code>ec2config</code>	<ul style="list-style-type: none"> • 'Service Start' • 'Ec2SetPassword' • 'Ec2HandleUserData' 	EC2Config <ul style="list-style-type: none"> • Service Start (Início do serviço): detecta se o serviço EC2Config está habilitado. • Ec2SetPassword: gera uma nova senha de administrador. • Ec2HandleUserData: permite que você execute um script de dados de usuário na próxima inicialização da instância.
<code>ec2launch</code>	'Reset Administrator Password'	Gera uma nova senha de administrador do Windows.
<code>network</code>	'DHCP Service Startup'	Interface de rede <ul style="list-style-type: none"> • DHCP Service Startup (Inicialização do serviço DHCP): detecta se o serviço DHCP está habilitado.

As seguintes opções estão disponíveis:

- `/level:<level>`: atributo opcional para o nível de verificação que a ação deve acionar. Os valores permitidos são: `information`, `warning`, `error`, `all`. Por padrão, ele é definido como `error`.
- `/check-only` atributo opcional que gera um relatório, mas não faz nenhuma modificação no volume offline.
- `/no-offline` atributo opcional que impede que o volume seja definido como offline após concluir a ação.
- `/no-fix-signature`: atributo opcional que não corrige uma possível colisão de assinatura de disco após concluir a ação.

Exemplos de salvamento

A seguir, exemplos usando a CLI do EC2Rescue for Windows Server. O volume é especificado usando o valor `device_id`.

Tentar corrigir todos os problemas identificados em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Tentar corrigir todos os problemas dentro de um grupo de serviço em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Tentar corrigir um item específico dentro de um grupo de serviço em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Especificar vários problemas para tentar corrigir em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Ação de restauração

O EC2Rescue for Windows Server pode detectar e resolver problemas com as seguintes configurações de serviço:

Grupo de serviço	Ações disponíveis	Descrição
Restaurar a última boa configuração conhecida	<code>lkgc</code>	Last Known Good Configuration (Última configuração válida conhecida): tenta inicializar a instância no estado inicializável mais recente conhecido.
Restaurar o registro do Windows do backup mais recente	<code>regback</code>	Restore registry from backup (Restaurar registro do backup): restaura o registro de <code>\Windows\System32\config\RegBack</code> .

As seguintes opções estão disponíveis:

- `/no-offline`—Atributo opcional que impede que o volume seja definido offline após concluir a ação.
- `/no-fix-signature`—Atributo opcional que não corrige uma possível colisão de assinatura de disco após concluir a ação.

Exemplos de restauração

A seguir, exemplos usando a CLI do EC2Rescue for Windows Server. O volume é especificado usando o valor device_id.

Restaurar a última boa configuração conhecida em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lgkc
```

Restaurar o último backup de registro do Windows em um volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Usar o EC2Rescue for Windows Server com o Run Command do Systems Manager

O AWS Support fornece um documento Run Command do Systems Manager para interagir com a instância habilitada para Systems Manager a fim de executar o EC2Rescue for Windows Server. O documento Run Command é chamado `AWSSupport-RunEC2RescueForWindowsTool`.

Este documento Run Command do Systems Manager realiza as seguintes tarefas:

- Baixa e verifica o EC2Rescue for Windows Server.
- Importa um módulo do PowerShell para facilitar a interação com a ferramenta.
- Executa EC2RescueCmd com o comando e os parâmetros fornecidos.

O documento Run Command do Systems Manager aceita três parâmetros:

- Comando—A EC2Rescue for Windows Server ação. Os valores atuais permitidos são:
 - ResetAccess—Restaura a senha do administrador local. A senha de administrador local da instância atual será restaurada e uma senha gerada aleatoriamente será armazenada com segurança no Parameter Store como `/EC2Rescue/Password/<INSTANCE_ID>`. Se você selecionar essa ação e não fornecer um parâmetro, as senhas serão criptografadas automaticamente com a chave padrão Chave do KMS. Opcionalmente, você pode especificar um ID de chave Chave do KMS em Parameters (Parâmetros) para criptografar a senha com sua própria chave.
 - CollectLogs—Executa o EC2Rescue for Windows Server com a ação `/collect:all`. Se você selecionar essa ação, `Parameters` deverá incluir um nome de bucket Amazon S3 no qual carregar os logs.
 - FixAll—Executa o EC2Rescue for Windows Server com a ação `/rescue:all`. Se você selecionar essa ação, `Parameters` deverá incluir o nome de dispositivo de bloco para salvar.
- Parameters—Os parâmetros do PowerShell para passar para o comando especificado.

Note

Para que a ação `ResetAccess` funcione, sua instância do Amazon EC2 precisa ter a seguinte política vinculada para gravar a senha criptografada no Parameter Store. Espere alguns minutos antes de tentar recuperar senha de uma instância depois de anexar essa política na função IAM relativa a ela.

Usando a Chave do KMS padrão:

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {
```

```
"Effect": "Allow",
"Action": [
    "ssm:PutParameter"
],
"Resource": [
    "arn:aws:ssm:region:account_id:parameter/EC2Rescue/Passwords/<instanceid>"
]
}
}
```

Usar uma Chave do KMS personalizada:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter"
            ],
            "Resource": [
                "arn:aws:ssm:region:account_id:parameter/EC2Rescue/Passwords/<instanceid>"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt"
            ],
            "Resource": [
                "arn:aws:kms:region:account_id:key/<kmskeyid>"
            ]
        }
    ]
}
```

O procedimento a seguir descreve como visualizar o JSON para este documento no console do Amazon EC2.

Para visualizar o JSON para o documento Run Command do Systems Manager

1. Abra o console do Systems Manager em <https://console.aws.amazon.com/systems-manager/home>.
2. No painel de navegação, expanda Shared Services e escolha Documents.
3. Na barra de pesquisa, defina o Proprietário como Meu ou da Amazon e defina o Prefixo de nome do documento como AWSSupport-RunEC2RescueForWindowsTool.
4. Selecione o documento AWSSupport-RunEC2RescueForWindowsTool, escolha Contents, e visualize o JSON.

Examples

Veja alguns exemplos sobre como usar o documento Run Command do Systems Manager para executar o EC2Rescue for Windows Server usando a AWS CLI. Para obter mais informações sobre o envio de comandos com a AWS CLI, consulte a [AWS CLI Command Reference](#) (Referências de comandos da AWS CLI).

Tentar corrigir todos os problemas identificados em um volume raiz offline

Tente corrigir todos os problemas identificados em um volume raiz off-line associado a uma instância do Windows do Amazon EC2:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue offline volume xvdf" --parameters "Command=FixAll, Parameters='xvdf'" --output text
```

Coletar logs da instância atual do Windows do Amazon EC2

Colete todos os logs da instância atual do Windows do Amazon EC2 online e carregue-os em um bucket do Amazon S3:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue online log collection to S3" --parameters "Command=CollectLogs, Parameters='YOURS3BUCKETNAME'" --output text
```

Coletar logs de um volume de instância do Windows do Amazon EC2 offline

Colete todos os logs de um volume offline associado a uma instância do Windows do Amazon EC2 e carregue-os no Amazon S3 com um URL pré-assinado:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue offline log collection to S3" --parameters "Command=CollectLogs, Parameters='\"-Offline -BlockDeviceName xvdf -S3PreSignedUrl YOURS3PRESIGNEDURL\"'" --output text
```

Redefinir a senha do administrador local

Os seguintes exemplos mostram os métodos que você pode usar para restaurar a senha de administrador local. A saída fornece um link para o Parameter Store, onde você encontra a senha segura gerada aleatoriamente para usar o RDP para sua instância do Windows do Amazon EC2 como administrador local.

Restaurar a senha de administrador local de uma instância online usando a chave padrão AWS KMS key alias/aws/ssm:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters "Command=ResetAccess" --output text
```

Restaurar a senha de administrador local de uma instância online usando uma Chave do KMS:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters "Command=ResetAccess, Parameters=a133dc3c-a2g4-4fc6-a873-6c0720104bf0" --output text
```

Note

Nesse exemplo, a Chave do KMS é a133dc3c-a2g4-4fc6-a873-6c0720104bf0.

EC2 Serial Console para instâncias do Windows

Com o console serial do EC2, você tem acesso à porta serial da instância do Amazon EC2, que pode ser usada para solucionar problemas de inicialização, configuração de rede e outros problemas. O console serial não exige que sua instância tenha recursos de rede. Com o console serial, você pode inserir comandos para uma instância como se o teclado e o monitor estivessem conectados diretamente à porta serial da instância. A sessão do console serial tem a duração do período de reinicialização e de parada

da instância. Durante a reinicialização, você pode visualizar todas as mensagens de inicialização desde o início.

O acesso ao console serial não está disponível por padrão. Sua organização deve conceder acesso da conta ao console serial e configurar políticas do IAM para conceder aos usuários acesso ao console serial. O acesso ao console serial pode ser controlado em um nível granular usando IDs de instância, tags de recursos e outras alavancas do IAM. Para obter mais informações, consulte [Configurar o acesso ao console serial do EC2 \(p. 1619\)](#).

O console serial pode ser acessado usando o console do EC2 ou a AWS CLI.

O console serial está disponível sem qualquer custo adicional.

Se você estiver usando uma instância do Linux, consulte [Console serial do EC2 para instâncias do Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Tópicos

- [Configurar o acesso ao console serial do EC2 \(p. 1619\)](#)
- [Conectar-se ao console serial do EC2 \(p. 1624\)](#)
- [Encerrar uma sessão do console serial do EC2 \(p. 1628\)](#)
- [Soluçinar problemas da instância do Windows usando o EC2 Serial Console \(p. 1629\)](#)

Configurar o acesso ao console serial do EC2

Para configurar o acesso ao console serial, você deve conceder acesso ao console serial no nível da conta e, em seguida, configurar políticas do IAM para conceder acesso aos usuários do IAM.

Tópicos

- [Níveis de acesso ao console serial do EC2 \(p. 1619\)](#)
- [Gerenciar o acesso da conta ao console serial do EC2 \(p. 1620\)](#)
- [Configurar políticas do IAM para acesso ao console serial do EC2 \(p. 1622\)](#)

Níveis de acesso ao console serial do EC2

Por padrão, não há acesso ao console serial no nível da conta. Você precisa explicitamente conceder acesso ao console serial no nível da conta. Para obter mais informações, consulte [Gerenciar o acesso da conta ao console serial do EC2 \(p. 1620\)](#).

Você pode usar uma política de controle de serviço (SCP) para permitir o acesso ao console serial dentro de sua organização. Em seguida, você pode ter controle de acesso granular no nível de usuário do IAM usando uma política do IAM para controlar o acesso. Usando uma combinação de políticas de SCP e do IAM, você tem diferentes níveis de controle de acesso ao console serial.

Nível da organização

Você pode usar uma política de controle de serviço (SCP) para permitir o acesso ao console serial para contas de membros dentro da sua organização. Para obter mais informações sobre SCPs, consulte [Service control policies](#) (Políticas de controle de serviço) no AWS Organizations User Guide (Manual do usuário do AWS Organizations).

Nível da instância

Você pode configurar as políticas de acesso ao console serial usando as construções IAM PrincipalTag e ResourceTag e especificando instâncias pelo ID delas. Para obter mais informações, consulte [Configurar políticas do IAM para acesso ao console serial do EC2 \(p. 1622\)](#).

Nível de usuário do IAM

Você pode configurar o acesso no nível do usuário configurando uma política do IAM para permitir ou negar a um usuário especificado a permissão para enviar a chave pública SSH ao serviço de console serial de uma instância específica. Para obter mais informações, consulte [Configurar políticas do IAM para acesso ao console serial do EC2 \(p. 1622\)](#).

Gerenciar o acesso da conta ao console serial do EC2

Por padrão, não há acesso ao console serial no nível da conta. Você precisa explicitamente conceder acesso ao console serial no nível da conta.

Tópicos

- [Conceder permissão aos usuários do IAM para gerenciar o acesso da conta \(p. 1620\)](#)
- [Exibir status de acesso da conta no console serial \(p. 1620\)](#)
- [Conceder acesso da conta ao console serial \(p. 1621\)](#)
- [Negar acesso da conta ao console serial \(p. 1621\)](#)

Conceder permissão aos usuários do IAM para gerenciar o acesso da conta

Para permitir que os usuários do IAM gerenciem o acesso da conta ao console serial do EC2, você precisa conceder a eles as permissões necessárias do IAM.

A política a seguir concede permissões para visualizar o status da conta e para permitir e impedir o acesso da conta ao console serial do EC2.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:GetSerialConsoleAccessStatus",  
                "ec2:EnableSerialConsoleAccess",  
                "ec2:DisableSerialConsoleAccess"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Para obter mais informações, consulte [Criar políticas do IAM](#) no Guia do usuário do IAM.

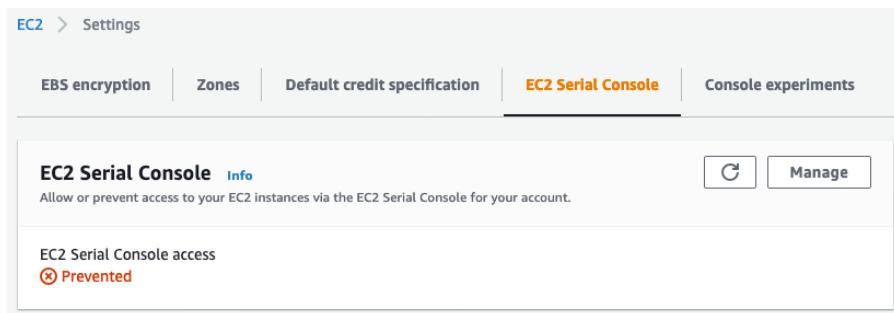
Exibir status de acesso da conta no console serial

Para exibir o status do acesso da conta no console serial (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos de conta), escolha EC2 Serial Console (Console serial do EC2).

O campo de acesso ao Console serial do EC2 indica se o acesso da conta é Allowed (Permitido) ou Prevented (Impedido).

A captura de tela a seguir mostra que a conta está impedida de usar o console serial do EC2.



Para exibir o status do acesso da conta ao console serial (AWS CLI)

Use o comando [get-serial-console-access-status](#) para exibir o status de acesso da conta ao console serial.

```
aws ec2 get-serial-console-access-status --region us-east-1
```

Na saída a seguir, true indica que a conta tem permissão para acessar o console serial.

```
{  
    "SerialConsoleAccessEnabled": true  
}
```

Conceder acesso da conta ao console serial

Para conceder acesso da conta ao console serial (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos de conta), escolha EC2 Serial Console (Console serial do EC2).
4. Escolha Gerenciar.
5. Para permitir acesso de todas as instâncias da conta ao console serial do EC2, marque a caixa de seleção Allow (Permitir).
6. Escolha Update.

Para conceder acesso da conta ao console serial (AWS CLI)

Use o comando [enable-serial-console-access](#) para permitir o acesso da conta ao console serial.

```
aws ec2 enable-serial-console-access --region us-east-1
```

Na saída a seguir, true indica que a conta tem permissão para acessar o console serial.

```
{  
    "SerialConsoleAccessEnabled": true  
}
```

Negar acesso da conta ao console serial

Para negar acesso da conta ao console serial (console)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

2. No painel de navegação, escolha EC2 Dashboard (Painel do EC2).
3. Em Account attributes (Atributos de conta), escolha EC2 Serial Console (Console serial do EC2).
4. Escolha Gerenciar.
5. Para evitar o acesso de todas as instâncias da conta ao console serial do EC2, desmarque a caixa de seleção Allow (Permitir).
6. Escolha Update.

Para negar acesso da conta ao console serial (AWS CLI)

Use o comando [disable-serial-console-access](#) para impedir o acesso da conta ao console serial.

```
aws ec2 disable-serial-console-access --region us-east-1
```

Na saída a seguir, `false` indica que a conta tem acesso negado ao console serial.

```
{  
    "SerialConsoleAccessEnabled": false  
}
```

Configurar políticas do IAM para acesso ao console serial do EC2

Por padrão, os usuários do IAM não têm acesso ao console serial. Sua organização deve configurar políticas do IAM para conceder aos usuários do IAM o acesso necessário. Para obter mais informações, consulte [Criar políticas do IAM](#) no Guia do usuário do IAM.

Para acessar o console serial, crie um documento de política JSON que inclua a ação `ec2-instance-connect:SendSerialConsoleSSH PublicKey`. Essa ação concede a um usuário do IAM permissão para enviar a chave pública para o serviço de console serial, que inicia uma sessão de console serial. Recomendamos restringir o acesso a instâncias do EC2 específicas. Caso contrário, todos os usuários do IAM com essa permissão poderão se conectar ao console serial de todas as instâncias do EC2.

Políticas de exemplo do IAM.

- [Permitir explicitamente o acesso ao console serial \(p. 1622\)](#)
- [Explicitamente negar acesso ao console serial \(p. 1623\)](#)
- [Usar tags de recursos para controlar o acesso ao console serial \(p. 1623\)](#)

Permitir explicitamente o acesso ao console serial

Por padrão, ninguém tem acesso ao console serial. Para conceder acesso ao console serial, é preciso configurar uma política para permitir explicitamente o acesso. Recomendamos configurar uma política que restrinja o acesso a instâncias específicas.

A política a seguir permite o acesso ao console serial de uma instância específica, identificada pelo ID da instância.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "AllowSerialConsoleAccess",  
            "Effect": "Allow",  
            "Action": [  
                "ec2-instance-connect:SendSerialConsoleSSH PublicKey"  
            ],  
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"  
        }  
    ]  
}
```

```
        }
    ]
```

Explicitamente negar acesso ao console serial

A política do IAM a seguir permite o acesso ao console serial de todas as instâncias, denotado pelo * (asterisco) e nega explicitamente o acesso ao console serial de uma instância específica, identificado por seu ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Usar tags de recursos para controlar o acesso ao console serial

Você pode usar tags de recursos para controlar o acesso ao console serial de uma instância.

O controle de acesso por atributo é uma estratégia de autorização que define permissões de acordo com tags que podem ser anexadas a usuários e a recursos da AWS. Por exemplo, a política a seguir permite que um usuário do IAM inicie uma conexão de console serial para uma instância somente se a tag de recurso desta instância e a tag da entidade principal tiverem o mesmo valor do SerialConsole para a chave de tag.

Para obter mais informações sobre como usar tags para controlar o acesso aos recursos da AWS, consulte [Controlling access to AWS resources](#) (Controlar o acesso aos recursos da AWS) no Guia do usuário do IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsoleSerialConsole}"
                }
            }
        }
    ]
}
```

]

Conectar-se ao console serial do EC2

Você pode se conectar ao console serial da instância do EC2 usando o console do Amazon EC2 ou por SSH. Depois de se conectar ao console serial, você pode usá-lo para solucionar problemas de inicialização, configuração de rede e outros problemas. Para obter mais informações sobre solução de problemas, consulte [Solucionar problemas da instância do Windows usando o EC2 Serial Console \(p. 1629\)](#).

Tópicos

- [Considerations \(p. 1624\)](#)
- [Prerequisites \(p. 1624\)](#)
- [Conectar-se ao console serial do EC2 \(p. 1625\)](#)
- [Impressões digitais do console serial EC2 \(p. 1627\)](#)

Considerations

- Apenas uma conexão de console serial ativa é suportada por instância.
- A conexão do console serial normalmente dura uma hora, a menos que você a encerre. No entanto, durante a manutenção do sistema, o Amazon EC2 encerrará a sessão do console serial.
- Demora 30 segundos para derrubar uma sessão depois que você se desconecta do console serial para permitir uma nova sessão.
- Porta de console serial suportada para Windows: COM1
- Quando você se conecta ao console serial, pode observar uma pequena queda na taxa de transferência da instância.

Prerequisites

- Compatível em todas as Regiões AWS, exceto África (Cidade do Cabo), Ásia-Pacífico (Hong Kong), Ásia-Pacífico (Osaka), China (Pequim), China (Ningxia), Europa (Milão) e Oriente Médio (Bahrein).
- Famílias de instâncias suportadas:
 - A1
 - C5, C5a, C5ad, C5d, C5n, C6g, C6gd
 - M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6g, M6gd
 - R5, R5a, R5ad, R5d, R5dn, R5n, R6, R6gd
 - T3, T3a, T4g
 - Z1d
- Configurar o acesso ao console serial do EC2
 - [Gerenciar o acesso da conta ao console serial do EC2 \(p. 1620\)](#).
 - [Configurar políticas do IAM para acesso ao console serial do EC2 \(p. 1622\)](#)Todos os usuários do IAM que usarão o console serial devem ter as permissões necessárias.
- Para se conectar ao console serialUsando o cliente com base em navegador (p. 1625), seu navegador deve suportar WebSocket. Se o navegador não suportar WebSocket, conecte-se ao console serialUsando sua própria chave e um cliente SSH. (p. 1625)
- A instância deve estar no estado pending, running, stopping ou shutting-down. Se a instância for terminated ou stopped, você não poderá se conectar ao console serial. Para obter mais informações sobre os estados da instância, consulte [Ciclo de vida da instância \(p. 412\)](#).

- Se a instância usar o Amazon EC2 Systems Manager, o SSM Agent versão 3.0.854.0 ou posterior deve ser instalado na instância. Para obter mais informações sobre o SSM Agent, consulte [Trabalhar com o SSM Agent](#) no Guia do usuário do AWS Systems Manager.

Você não precisa de um servidor sshd instalado ou em execução na sua instância.

Conectar-se ao console serial do EC2

Opções de conexão

- [Conectar-se usando o cliente com base em navegador \(p. 1625\)](#)
- [Conectar-se usando sua própria chave e cliente SSH \(p. 1625\)](#)

Conectar-se usando o cliente com base em navegador

Você pode se conectar ao console serial da instância do EC2 usando o cliente com base em navegador. Faça isso selecionando a instância no console do Amazon EC2 e escolhendo conectar-se ao console serial. O cliente com base em navegador lida com as permissões e fornece uma conexão bem-sucedida.

O console serial do EC2 funciona a na maioria dos navegadores e suporta entrada de teclado e mouse.

Para se conectar à porta serial da instância usando o cliente com base em navegador (console do Amazon EC2)

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).
3. Selecione a instância e escolha Connect (Conectar), EC2 Serial Console (Console serial do EC2), Connect (Conectar).

Como alternativa, você pode selecionar a instância e escolher Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), EC2 Serial Console (Console serial do EC2), Connect (Conectar).

Uma janela de terminal no navegador é aberta.

4. Pressione Enter. Se for exibido um prompt de login, significará que você está conectado ao console serial.

Se a tela permanecer preta, você poderá usar as seguintes informações para ajudar a resolver problemas com a conexão ao console serial:

- Verifique se você configurou o acesso ao console serial. Para obter mais informações, consulte [Configurar o acesso ao console serial do EC2 \(p. 1619\)](#).
- Reinicie a instância. Você pode reiniciar sua instância usando o o console do EC2 ou aAWS CLI. Para obter mais informações, consulte [Reinicializar a instância \(p. 470\)](#).

Conectar-se usando sua própria chave e cliente SSH

Você pode usar sua própria chave do SSH e conectar-se à sua instância a partir do cliente SSH de sua escolha enquanto usa a API do console serial. Isso permite que você se beneficie da capacidade do console serial de enviar por push uma chave pública para a instância.

Para se conectar ao console serial de uma instância usando SSH

1. Envie por push a chave pública do SSH para a instância para iniciar uma sessão de console serial

Use o comando [send-serial-console-ssh-public-key](#) para enviar por push a chave pública do SSH para a instância. Isso inicia uma sessão de console serial.

Se uma sessão de console serial já tiver sido iniciada para essa instância, o comando falhará porque você só pode ter uma sessão aberta de cada vez. Demora 30 segundos para derrubar uma sessão depois que você se desconecta do console serial para permitir uma nova sessão.

```
C:\> aws ec2-instance-connect send-serial-console-ssh-public-key \
--instance-id i-001234a4bf70dec41EXAMPLE \
--serial-port 0 \
--ssh-public-key file://my_rsa_key.pub \
--region us-east-1
```

2. Conecte-se ao console serial usando sua chave privada

Use o comando ssh para se conectar ao console serial antes que a chave pública seja removida do serviço de console serial. Você tem 60 segundos antes que ela seja removida.

Use a chave privada que corresponde à chave pública.

O formato do nome de usuário é `instance-id.port0`, que abrange o ID da instância e a porta 0. No exemplo a seguir, o nome de usuário é `i-001234a4bf70dec41EXAMPLE.port0`.

Para todas as Regiões AWS compatíveis, exceto as Regiões AWS GovCloud (US) :

O formato do nome DNS público do serviço de console serial é `serial-console.ec2-instance-connect.region.amazonaws.com`. No exemplo a seguir, o serviço de console serial está na região `us-east-1`.

```
C:\> ssh -i my_rsa_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-
connect.us-east-1.amazonaws.com
```

Somente para Regiões AWS GovCloud (US) :

O formato do nome DNS público do serviço de console serial nas regiões AWS GovCloud (US) é `serial-console.ec2-instance-connect.GovCloud-region.amazonaws.com`. No exemplo a seguir, o serviço de console serial está na região `us-east-1`.

```
C:\> ssh -i my_rsa_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-
connect.us-gov-east-1.amazonaws.com
```

3. (Opcional) Verificar a impressão digital

Quando você se conecta pela primeira vez ao console serial, é solicitado a verificar a impressão digital. Você pode comparar a impressão digital do console serial com a impressão digital exibida para verificação. Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se elas corresponderem, você poderá se conectar com confiança ao console serial.

A seguinte impressão digital corresponde ao serviço de console serial na região us-east-1. Para obter as impressões digitais de cada região, consulte [Impressões digitais do console serial EC2 \(p. 1627\)](#).

```
SHA256:dXwn5ma/xadVMeBZGERu5l2gx+yI5LDiJaLUCz0FMmw
```

Note

A impressão digital só aparece na primeira vez que você se conecta ao console serial.

4. Pressione Enter. Se for exibido um prompt, significará que você está conectado ao console serial.

Se a tela permanecer preta, você poderá usar as seguintes informações para ajudar a resolver problemas com a conexão ao console serial:

- Verifique se você configurou o acesso ao console serial. Para obter mais informações, consulte [Configurar o acesso ao console serial do EC2 \(p. 1619\)](#).
- Reinicie a instância. Você pode reiniciar sua instância usando o o console do EC2 ou aAWS CLI. Para obter mais informações, consulte [Reinicializar a instância \(p. 470\)](#).

Impressões digitais do console serial EC2

A impressão digital do console serial do EC2 é exclusiva para cada região da AWS.

- us-east-1 – Leste dos EUA (Norte da Virgínia)

```
SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUCz0FMmw
```

- us-east-2 – Leste dos EUA (Ohio)

```
SHA256:EhwPkTzRtTY7TRSzz26XbB0/HvV9jRM7mCZN0xw/d/0
```

- us-west-1: Oeste dos EUA (Norte da Califórnia)

```
SHA256:OHldlcMET8u7QLSX3jmRTRAPFHvtqbyoLZBMUCqiH3Y
```

- us-west-2 – Oeste dos EUA (Oregon)

```
SHA256:EMCIe23TqKaBI6yGHainqZcMwqNkDhhAVHa1O2JxVUc
```

- ap-south-1: Ásia-Pacífico (Mumbai)

```
SHA256:oBLXcYmk1qHHEbliARxEgH8Is051rezTPiSM35BsU40
```

- ap-northeast-2: Ásia-Pacífico (Seul)

```
SHA256:FoqWXNX+DZ++GuNTztg9PK49WYMqBX+FrcZM2dSrqrI
```

- ap-southeast-1 – Ásia-Pacífico (Singapura)

```
SHA256:PLFNn7WnCQDHx3qmwLu1Gy/08TUX7LQgZuaC6L45CoY
```

- ap-southeast-2 – Ásia-Pacífico (Sydney)

```
SHA256:yFvMwUK91EUQjQTRoXXzuN+cW9/VSe9W984Cf5Tgzo4
```

- ap-northeast-1 – Ásia-Pacífico (Tóquio)

```
SHA256:RQfsDCZTOFQawewTRDV1t9Em/HMrFQe+CRLIOT5um4k
```

- ca-central-1: Canadá (Central)

```
SHA256:P202jOZwmpMwkp06YW738FIOTHdUTyEv2gczYMMO7s4
```

- eu-central-1 – Europa (Frankfurt)

```
SHA256:aCMFS/yIcOd0lkXv0l8AmZ1Toe+bBnrJJ3Fy0k0De2c
```

- eu-west-1 – Europa (Irlanda)

```
SHA256:h2AaGAWO4Hathhtm6ezs3Bj7udgUxi2qTrHjZAwCW6E
```

- eu-west-2: Europa (Londres)

```
SHA256:a69rd5CE/AEG4Amm53I6lkD1ZPvS/BCV3tTPW2RnJg8
```

- eu-west-3: Europa (Paris)

```
SHA256:q81dnAf9pymeNe8BnFVngY3RPAr/kxswJUzfrlxewS
```

- eu-north-1: Europa (Estocolmo)

```
SHA256:tkGFFUVUDvocDiGSS3Cu8Gdl6w2uI32EPNpKFKLwX84
```

- sa-east-1: América do Sul (São Paulo)

```
SHA256:rd2+/320gnjew1yVIemENaQzC+Botbih620qAPDq1dI
```

- us-gov-east-1: AWS GovCloud (Leste dos EUA)

```
SHA256:tIwe19GWsoyLC1rtvu38YEEh+DHIkqnDcZnmtebvF28
```

- us-gov-west-1: AWS GovCloud (Oeste dos EUA)

```
SHA256:kfOFRWLaoZfB+utbd3bRf801Pf8nGO2YZLqXziiIw5DQ
```

Encerrar uma sessão do console serial do EC2

A maneira de encerrar uma sessão de console serial depende do cliente.

Cliente com base em navegador

Para encerrar a sessão do console serial, feche a janela de terminal no navegador do console serial.

Cliente OpenSSH padrão

Para encerrar a sessão do console serial, use o comando a seguir para fechar a conexão SSH. Esse comando deve ser executado imediatamente após uma nova linha.

```
C:\> ~.
```

Note

O comando que você usa para fechar uma conexão SSH pode ser diferente, dependendo do cliente SSH que você está usando.

Solucionar problemas da instância do Windows usando o EC2 Serial Console

Ao usar o console serial do EC2, você pode solucionar problemas de inicialização, configuração de rede e outros problemas ao se conectar à porta serial da instância.

Tópicos

- [Usar o SAC para solucionar problemas de instâncias do Windows \(p. 1629\)](#)

Para obter informações sobre como solucionar problemas de instâncias do Linux, consulte [Solucionar problemas de instâncias do Linux usando o console serial do EC2](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Usar o SAC para solucionar problemas de instâncias do Windows

O recurso Special Admin Console (SAC) do Windows fornece uma maneira de solucionar problemas de uma instância do Windows. Ao se conectar ao console serial da instância e usando o SAC, você pode interromper o processo de inicialização e inicializar o Windows no modo de segurança.

Tópicos

- [Limitations \(p. 1629\)](#)
- [Prerequisites \(p. 1629\)](#)
- [Usar o SAC \(p. 1630\)](#)
- [Usar o menu de inicialização \(p. 1632\)](#)

Limitations

Se você executar uma instância com uma AMI pré-configurada com o SAC, os serviços do EC2 que dependem de recuperação de senha não funcionarão no console.

Prerequisites

Para usar o SAC para solucionar problemas de uma instância do Windows, você deve primeiro concluir os seguintes pré-requisitos:

1. Conceda acesso ao console serial. Para obter mais informações, consulte [Configurar o acesso ao console serial do EC2 \(p. 1619\)](#).
2. Habilite o SAC e o menu de inicialização. Para obter mais informações, consulte [Habilitar o SAC e o menu de inicialização \(p. 1629\)](#).
3. Conecte-se ao console serial. Para obter mais informações, consulte [Conectar-se ao console serial do EC2 \(p. 1624\)](#).

Habilitar o SAC e o menu de inicialização

Use um dos métodos a seguir para habilitar o SAC e o menu de inicialização em uma instância.

PowerShell

Para habilitar o SAC e o menu de inicialização em uma instância do Windows

1. [Conecte-se \(p. 443\)](#) à sua instância e execute as seguintes etapas na linha de comando do PowerShell.

-
2. Habilite o SAC.

```
bcdedit /ems '{current}' on  
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Habilite o menu de inicialização.

```
bcdedit /set '{bootmgr}' displaybootmenu yes  
bcdedit /set '{bootmgr}' timeout 15  
bcdedit /set '{bootmgr}' bootebris yes
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Command prompt

Para habilitar o SAC e o menu de inicialização em uma instância do Windows

1. [Conecte-se \(p. 443\)](#) à sua instância e execute as seguintes etapas no prompt de comando.
2. Habilite o SAC.

```
bcdedit /ems {current} on  
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Habilite o menu de inicialização.

```
bcdedit /set {bootmgr} displaybootmenu yes  
bcdedit /set {bootmgr} timeout 15  
bcdedit /set {bootmgr} bootebris yes
```

4. Aplique a configuração atualizada reinicializando a instância.

```
shutdown -r -t 0
```

Usar o SAC

Para usar o SAC

1. [Conecte-se ao console serial. \(p. 1624\)](#)

Se o SAC estiver habilitado na instância, o console serial exibirá OSAC>editor.exe?".

```
Computer is booting, SAC started and initialized.  
Use the "ch -?" command for information about using channels.  
Use the "?" command for general help.  
  
SAC>?  
EVENT: The CMD command is now available.  
SAC_
```

2. Para exibir os comandos do SAC, digite?E pressioneDigite.

Saída esperada

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Solucionar problemas da instância
usando o console Serial do EC2

```
SAC>?  
ch          Channel management commands. Use ch -? for more help.  
cmd         Create a Command Prompt channel.  
d           Dump the current kernel log.  
f           Toggle detailed or abbreviated tlist info.  
? or help   Display this list.  
i <#> <ip> <subnet> <gateway> Set IPv4 addr., subnet and gateway.  
id          Display the computer identification information.  
k <pid>    Kill the given process.  
l <pid>    Lower the priority of a process to the lowest possible.  
lock        Lock access to Command Prompt channels.  
m <pid> <MB-allow> Limit the memory usage of a process to <MB-allow>.  
p           Toggle paging the display.  
r <pid>    Raise the priority of a process by one.  
s           Display the current time and date (24 hour clock used).  
s mm/dd/yyyy hh:mm  Set the current time and date (24 hour clock used).  
t           Tlist.  
restart     Restart the system immediately.  
shutdown   Shutdown the system immediately.  
crashdump  Crash the system. You must have crash dump enabled.
```

3. Para criar um canal de linha de comandos (comocmd0001oucmd0002), insira cmdE pressione Digite.
4. Para ver o canal do prompt de comando, pressione ESC pressione TAB.

Saída esperada

```
Name:          Cmd0001  
Description:   Command  
Type:         VT-UTF8  
Channel GUID: ef9f20a0-1287-11eb-82b0-0e4ba51872e5  
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0  
  
Press <esc><tab> for next channel.  
Press <esc><tab>0 to return to the SAC channel.  
Use any other key to view this channel.
```

5. Para trocar de canais, pressione ESC+tab+número do canal junto. Por exemplo, para alternar para o cmd0002 (se tiver sido criado), pressione ESC+TABA+2.
6. Insira as credenciais exigidas pelo canal do prompt de comando.

```
Please enter login credentials.  
Username: Administrator  
Domain : .  
Password: *****
```

O prompt de comando é o mesmo shell de comando completo que você obtém em um desktop, mas com a exceção de que ele não permite a leitura de caracteres que já foram emitidos.

```
Microsoft Windows [Version 10.0.17763.1457]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>diskpart  
  
Microsoft DiskPart version 10.0.17763.1  
  
Copyright (C) Microsoft Corporation.  
On computer: EC2AMAZ-ASR4SAI  
  
DISKPART> list disk  
  
Disk ##  Status       Size     Free      Dyn  Gpt  
-----  -----  
Disk 0   Online       30 GB    0 B      ---  ---  
Disk 1   Online       46 GB    46 GB    ---  ---  
  
DISKPART> -
```

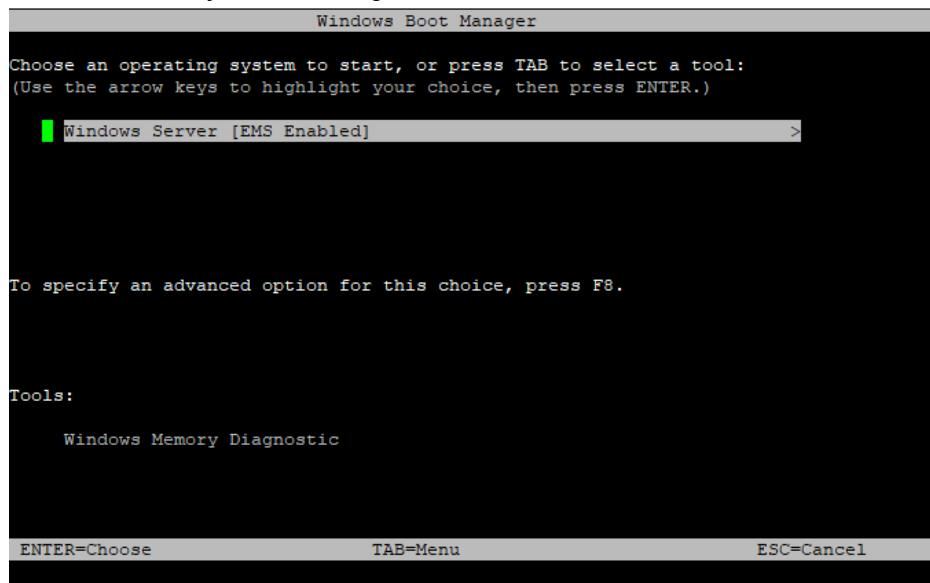
O PowerShell também pode ser usado a partir do prompt de comando.

Observe que talvez seja necessário definir a preferência do progresso para o modo silencioso.

```
PS C:\Windows\system32> $ProgressPreference="SilentlyContinue"
PS C:\Windows\system32> $computerInfo = Get-ComputerInfo
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Name
Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Description
Intel64 Family 6 Model 85 Stepping 4
PS C:\Windows\system32> -
```

Usar o menu de inicialização

Se a instância tiver o menu de inicialização habilitado e for reiniciado após a conexão via SSH, você verá o menu de inicialização, como a seguir.



Comandos do menu de inicialização

ENTER

Inicia a entrada selecionada do sistema operacional.

TAB

Altera para o menu Tools (Ferramentas).

ESC

Cancela e reinicia a instância.

ESC seguido por 8

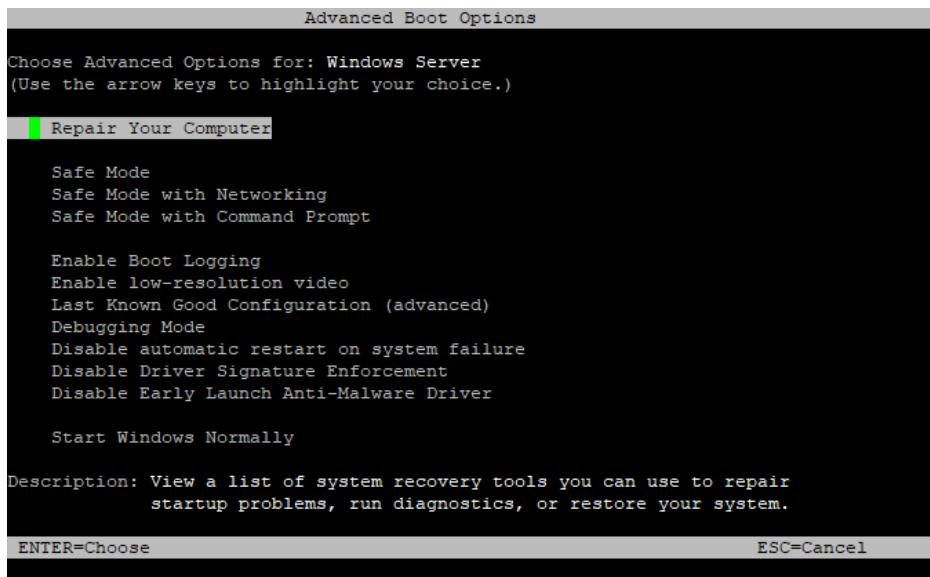
Equivalentе a pressionar F8. Mostra opções avançadas para o item selecionado.

Tecla ESC + seta para a esquerda

Volta para o menu de inicialização inicial.

Note

A tecla ESC por si só não leva você de volta ao menu principal porque o Windows está aguardando para ver se uma sequência de escape está em andamento.



Enviar uma interrupção para diagnóstico (para usuários avançados)

Warning

As interrupções de diagnóstico são destinadas ao uso de usuários avançados. O uso incorreto pode ter um impacto negativo sobre sua instância. Enviar uma interrupção de diagnóstico para uma instância pode acionar uma instância para travar e reinicializar, o que pode levar à perda de dados.

Você pode enviar uma interrupção para diagnóstico a uma instância inacessível ou sem resposta do Windows para acionar manualmente um erro de parada. Os erros de parada normalmente são referenciados como erros de tela azul.

Em geral, os sistemas operacionais Windows falham e reinicializam quando ocorre um erro de parada, mas o comportamento específico depende de sua configuração. Um erro de parada também pode fazer com que o sistema operacional grave informações de depuração, como um despejo de memória de kernel, em um arquivo. É possível usar essas informações para conduzir análises de causa raiz para depurar a instância.

Os dados do despejo da memória são gerados localmente pelo sistema operacional na própria instância.

Antes de enviar uma interrupção de diagnóstico para sua instância, recomendamos que você consulte a documentação do seu sistema operacional e, em seguida, faça as alterações de configuração necessárias.

Tópicos

- [Tipos de instâncias compatíveis \(p. 1634\)](#)
- [Prerequisites \(p. 1634\)](#)
- [Enviar uma interrupção para diagnóstico \(p. 1634\)](#)

Tipos de instâncias compatíveis

A interrupção do diagnóstico é compatível com todos os tipos de instância baseadas em Nitro, exceto A1. Para obter mais informações, consulte [Instâncias criadas no Sistema Nitro \(p. 154\)](#).

Prerequisites

Antes de usar uma interrupção para diagnóstico, configure o sistema operacional da instância para executar as ações necessárias quando ocorrer um erro de parada.

Para configurar o Windows para gerar um despejo de memória quando ocorrer um erro de parada.

1. Conecte-se à sua instância.
2. Abra o Control Panel (Painel de controle) e escolha System (Sistema), Advanced system settings (Configurações avançadas do sistema).
3. Na caixa de diálogo System Properties (Propriedades do sistema), escolha a guia Advanced (Avançado).
4. Na seção Startup and Recovery (Inicialização e recuperação), escolha Settings... (Configurações...).
5. Na seção System failure (Falha do sistema), defina as configurações conforme necessário e escolha OK.

Para obter mais informações sobre como configurar os erros de parada do Windows, consulte [Visão geral das opções do arquivo de despejo de memória do Windows](#).

Enviar uma interrupção para diagnóstico

Depois de concluir as alterações necessárias na configuração, você pode enviar uma interrupção para diagnóstico para sua instância usando a AWS CLI ou a API do Amazon EC2.

Para enviar uma interrupção para diagnóstico para sua instância (AWS CLI)

Use o comando `send-diagnostic-interrupt` e especifique o ID da instância.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

Para enviar uma interrupção para diagnóstico para sua instância (AWS Tools for Windows PowerShell)

Use o cmdlet `Send-EC2DiagnosticInterrupt` e especifique o ID da instância.

```
PS C:\> Send-EC2DiagnosticInterrupt-InstanceId i-1234567890abcdef0
```

Problemas comuns com instâncias do Windows

Veja a seguir dicas de solução de problemas para ajudar a resolver problemas comuns com a instância do EC2 executando o Windows Server.

Problemas

- [Os volumes do EBS não são inicializados no Windows Server 2016 e posterior \(p. 1635\)](#)
- [Inicialize uma instância do EC2 Windows no Directory Services Restore Mode \(DSRM\) \(p. 1635\)](#)
- [A instância perde a conectividade de rede ou as tarefas agendadas não são executadas quando esperado \(p. 1637\)](#)

-
- [Não foi possível obter o resultado do console \(p. 1638\)](#)
 - [Windows Server 2012 R2 não disponível na rede \(p. 1638\)](#)

Os volumes do EBS não são inicializados no Windows Server 2016 e posterior

Instâncias criadas nas Imagens de máquina da Amazon (AMIs) para Windows Server 2016 e posterior usam o serviço EC2Launch para uma variedade de tarefas de inicialização, incluindo a inicialização de volumes do EBS. Por padrão, o EC2Launch não inicializa volumes secundários. Configure o EC2Launch para inicializar esses discos automaticamente.

Para mapear letras de unidade a volumes

1. Conecte-se à instância para configurar e abrir o arquivo C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json em um editor de texto.
2. Especifique as configurações de volume usando o seguinte formato:

```
{  
  "driveLetterMapping": [  
    {  
      "volumeName": "sample volume",  
      "driveLetter": "H"  
    }  
  ]  
}
```

3. Salve as alterações e feche o arquivo.
4. Abra o Windows PowerShell e use o seguinte comando para executar o script do EC2Launch que inicializa os discos:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Para inicializar os discos sempre que a instância for inicializada, adicione o sinalizador –Schedule da seguinte forma:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -Schedule
```

Initialize uma instância do EC2 Windows no Directory Services Restore Mode (DSRM)

Se uma instância que estiver executando o Microsoft Active Directory tiver uma falha do sistema ou outros problemas críticos, você poderá solucionar problemas na instância inicializando em uma versão especial do modo seguro denominado Directory Services Restore Mode (DSRM). No DSRM, você pode reparar ou recuperar o Ative Directory.

Suporte a drivers para DSRM

A forma como você habilita o DSRM e faz a inicialização na instância depende dos drivers que a instância estiver executando. No console do EC2, você pode visualizar os detalhes de versão do driver para uma instância no log do sistema. As tabelas a seguir mostram quais drivers são compatíveis com o DSRM.

Versões do driver	DSRM com suporte?	Próximas etapas
Citrix PV 5.9	Não	Restaure a instância de um backup. Você não pode habilitar o DSRM.
AWS PV 7.2.0	Não	Embora o DSRM não tenha suporte para esse driver, você ainda pode desanexar o volume raiz da instância, criar um snapshot do volume ou criar uma AMI dele e anexá-la a outra instância na mesma zona de disponibilidade que um volume secundário. Em seguida, você pode habilitar o DSRM (como descrito nesta seção).
AWS PV 7.2.2 e posterior	Sim	Desanexe o volume raiz, anexe-o a outra instância e habilite o DSRM (como descrito nesta seção).
Redes avançadas	Sim	Desanexe o volume raiz, anexe-o a outra instância e habilite o DSRM (como descrito nesta seção).

Para obter informações sobre como habilitar as redes aprimoradas, consulte [Como habilitar as redes aprimoradas em instâncias Windows em uma VPC](#). Para obter mais informações sobre como atualizar os drivers AWS PV, consulte [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#).

Configurar uma instância para ser inicializada no DSRM

As instâncias do EC2 Windows não têm conectividade de rede antes que o sistema operacional seja executado. Por esse motivo, você não pode pressionar o botão F8 no teclado para selecionar uma opção de inicialização. Você deve usar um dos seguintes procedimentos para inicializar uma instância do EC2 Windows Server no DSRM.

Se você suspeitar que o Active Directory foi danificado e a instância ainda estiver em execução, você poderá configurar a instância para fazer a inicialização no DSRM usando a caixa de diálogo Configurações do sistema ou o prompt de comando.

Para inicializar uma instância online no DSRM usando a caixa de diálogo Configurações do sistema

1. Na caixa de diálogo Executar, digite `msconfig` e pressione Enter.
2. Escolha a guia Iniciar.
3. Em Opções de inicialização, escolha Inicialização segura.
4. Escolha Reparo do Active Directory e escolha OK. O sistema solicita que você reinicialize o servidor.

Para inicializar uma instância online no DSRM usando a linha de comando

Em uma janela do prompt de comando, execute o comando a seguir:

```
bcdedit /set safeboot dsrepair
```

Se uma instância estiver offline e inacessível, você deverá desanexar o volume raiz e anexá-lo a outra instância para habilitar o modo DSRM.

Para inicializar uma instância offline no DSRM

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.

-
2. No painel de navegação, escolha Instances (Instâncias).
 3. Localize e selecione a instância afetada. Escolha Instance state (Estado da instância) e Stop instance (Interromper instância).
 4. Escolha Launch instances (Executar instância) e crie uma instância temporária na mesma zona de disponibilidade que a instância afetada. Escolha um tipo de instância que use uma versão diferente do Windows. Por exemplo, se sua instância for Windows Server 2008, escolha uma instância Windows Server 2008 R2.

Important

Se você não criar a instância na mesma zona de disponibilidade que a instância afetada, não conseguirá associar o volume do dispositivo raiz da instância afetada à nova instância.

5. No painel de navegação, escolha Volumes.
6. Localize o volume do dispositivo raiz da instância afetada. [Separe](#) o volume e [associe-o](#) à instância temporária criada anteriormente. Associe-a com o nome do padrão do dispositivo (xvdf).
7. Use a Área de Trabalho Remota para conectar-se à instância temporária e use em utilitário Gerenciamento de Disco para [disponibilizar o volume para uso](#).
8. Abra um prompt de comando e execute o seguinte comando. Substitua D pela letra real de unidade do volume secundário que você acabou de anexar:

```
bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
```

9. No utilitário de Gerenciamento de Disco, escolha a unidade que você associou anteriormente, abra o menu contextual (botão direito do mouse) e escolha Offline.
10. No console do EC2, separe o volume afetado de instância temporária e reanexe-o à sua instância original com o nome de dispositivo /dev/sda1. Você deve especificar o nome desse dispositivo para designar o volume como volume do dispositivo raiz.
11. [Inicie](#) a instância.
12. Depois que a instância passar nas verificações de integridade no console do EC2, conecte-se à instância usando o Remote Desktop e verifique se ela é inicializada no modo DSRM.
13. (Opcional) Exclua ou interrompa a instância temporária que você criou nesse procedimento.

A instância perde a conectividade de rede ou as tarefas agendadas não são executadas quando esperado

Se você reiniciar sua instância e perder a conectividade de rede, é possível que a instância tenha o horário errado.

Por padrão, as instâncias do Windows usam o tempo universal coordenado (UTC). Se você definir o horário de sua instância como outro fuso horário e, em seguida, reiniciá-la, ocorrerá um desvio no horário, e a instância perderá temporariamente seu endereço IP. A instância recuperará a conectividade de rede, mas isso pode levar várias horas. A quantidade de tempo que leva para a instância recuperar a rede de conectividade depende da diferença entre o UTC e o outro fuso horário.

Esse mesmo problema no horário também pode fazer com que as tarefas agendadas não sejam executadas no horário esperado. Nesse caso, as tarefas agendadas não são executadas quando esperado porque a instância tem o horário incorreto.

Para usar um fuso horário diferente do UTC de forma persistente, você deve definir a chave de Registro RealTimelsUniversal. Sem essa chave, a instância usará o UTC depois de reiniciá-la.

Para resolver problemas no horário que causam a perda da conectividade de rede

1. Certifique-se de que você esteja executando os drivers PV recomendados. Para obter mais informações, consulte [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#).
2. Verifique se a chave de Registro a seguir existe e está definida como 1: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimelsUniversal

Não foi possível obter o resultado do console

Para instâncias do Windows, o console da instância exibe o resultado das tarefas realizadas durante o processo de inicialização do Windows. Se o Windows for inicializado com êxito, a última mensagem registrada será `Windows is Ready to use`. Você também pode exibir mensagens do log de eventos no console, mas esse recurso não é habilitado por padrão. Para obter mais informações, consulte [Propriedades do serviço do EC2 \(p. 534\)](#).

Para obter a saída do console da instância usando o console do Amazon EC2, selecione a instância e escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema). Para obter a saída do console usando a linha de comando, use um dos seguintes comandos: `get-console-output` (AWS CLI) ou `Get-EC2ConsoleOutput` (AWS Tools for Windows PowerShell).

Para instâncias executadas no Windows Server 2012 R2 e anteriores, se a saída do console estiver vazia, poderá indicar um problema com o serviço EC2Config, como um arquivo de configuração desconfigurado ou que o Windows não foi inicializado corretamente. Para corrigir o problema, faça download e instale a versão mais recente do EC2Config. Para obter mais informações, consulte [Instalar a versão mais recente do EC2Config \(p. 532\)](#).

Windows Server 2012 R2 não disponível na rede

Para obter informações sobre como solucionar problemas de uma instância Windows Server 2012 R2 que não está disponível na rede, consulte [O Windows Server 2012 R2 perde a conectividade de rede e armazenamento após a reinicialização de uma instância \(p. 571\)](#).

Mensagens comuns na solução de problemas de instâncias Windows

Esta seção inclui dicas para ajudar a solucionar problemas com base em mensagens comuns.

Tópicos

- "A senha não está disponível" (p. 1639)
- "A senha ainda não está disponível" (p. 1639)
- "Não é possível recuperar a senha do Windows" (p. 1639)
- "Esperando o serviço de metadados" (p. 1640)
- "Não é possível ativar o Windows" (p. 1642)
- "O Windows não é genuíno (0x80070005)" (p. 1644)
- "Nenhum servidor de licença do servidor terminal disponível para fornecer uma licença" (p. 1644)
- "Algumas configurações são gerenciadas pela sua organização" (p. 1645)

"A senha não está disponível"

Para conectar-se a uma instância Windows usando Remote Desktop, você deve especificar uma conta e uma senha. As contas e as senhas são fornecidas com base na AMI usada para executar a instância. Você pode recuperar a senha gerada automaticamente para a conta de administrador ou usar a conta e a senha que estavam em uso na instância original na qual a AMI foi criada.

Se sua instância Windows não estiver configurada para gerar uma senha aleatória, você receberá a seguinte mensagem quando recuperar a senha gerada automaticamente usando o console:

```
Password is not available.  
The instance was launched from a custom AMI, or the default password has changed. A  
password cannot be retrieved for this instance. If you have forgotten your password, you  
can  
reset it using the Amazon EC2 configuration service. For more information, see Passwords  
for a  
Windows Server instance.
```

Verifique a saída do console relativa à instância para ver se a AMI usada para executá-la foi criada com a geração de senha desabilitada. Se a geração de senha estiver desabilitada, a saída do console conterá o seguinte:

```
Ec2SetPassword: Disabled
```

Se a geração de senha estiver desabilitada e não se lembrar da senha da instância original, você poderá redefinir a senha para essa instância. Para obter mais informações, consulte [Redefinir uma senha de administrador do Windows perdida ou expirada \(p. 1590\)](#).

"A senha ainda não está disponível"

Para conectar-se a uma instância Windows usando Remote Desktop, você deve especificar uma conta e uma senha. As contas e as senhas são fornecidas com base na AMI usada para executar a instância. Você pode recuperar a senha gerada automaticamente para a conta de administrador ou usar a conta e a senha que estavam em uso na instância original na qual a AMI foi criada.

A senha deve estar disponível em instantes. Se a senha não estiver disponível, você receberá a seguinte mensagem quando recuperar a senha gerada automaticamente usando o console:

```
Password not available yet.  
Please wait at least 4 minutes after launching an instance before trying to retrieve the  
auto-generated password.
```

Se demorar mais do que quatro minutos e você ainda não conseguir obter a senha, é possível que o EC2Config está desabilitado. Verifique se a saída do console está vazia. Para obter mais informações, consulte [Não foi possível obter o resultado do console \(p. 1638\)](#).

Verifique também se a conta do AWS Identity and Access Management (IAM) que está sendo usada para acessar o Portal de Gerenciamento tem a ação `ec2:GetPasswordData` permitida. Para obter mais informações sobre as permissões do IAM, consulte [O que é IAM?](#).

"Não é possível recuperar a senha do Windows"

Para recuperar a senha gerada automaticamente para a conta de administrador, você deve usar a chave privada para o par de chaves que você especificou ao executar a instância. Se você não tiver especificado um par de chaves quando executou a instância, você receberá a seguinte mensagem.

Cannot retrieve Windows password

Você pode encerrar essa instância e executar uma nova instância usando a mesma AMI, certificando-se de especificar um par de chaves.

"Esperando o serviço de metadados"

Uma instância Windows deve obter informações dos metadados de sua instância para poder se ativar. Por padrão, a configuração `WaitForMetaDataAvailable` assegura que o serviço EC2Config aguardará que os metadados da instância fiquem acessíveis antes de continuar com o processo de inicialização. Para obter mais informações, consulte [Metadados da instância e dados do usuário \(p. 622\)](#).

Se a instância falhar no teste de acessibilidade, experimente o seguinte para resolver o problema.

- Verifique o bloco CIDR de sua VPC. Uma instância Windows não pode ser inicializada corretamente se for executada em uma VPC com um intervalo de endereços IP de 224.0.0.0 a 255.255.255.255 (intervalos de endereços IP de classe D e classe E). Esses intervalos de endereços IP são reservados e não devem ser atribuídos a dispositivos de host. Recomendamos criar uma VPC com um bloco CIDR dos intervalos de endereços IP (não roteáveis publicamente) privados especificados na [RFC 1918](#).
- É possível que o sistema foi configurado com um endereço IP estático. Tente [criar uma interface de rede \(p. 1015\)](#) e [anexá-la à instância \(p. 1017\)](#).
- Para habilitar o DHCP em uma instância Windows à qual você não pode se conectar
 1. Interrompa a instância afeta e desanexe seu volume raiz.
 2. Execute uma instância temporária na mesma zona de disponibilidade que a instância afetada.

Warning

Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas adicionais ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco. Como alternativa, selecione uma AMI diferente para a instância temporária. Por exemplo, se a instância original usar a AMI Windows da AWS para Windows Server 2008 R2, execute a instância temporária usando uma AMI Windows da AWS para Windows Server 2012.

3. Anexe o volume raiz da instância afetada a essa instância temporária. Conecte-se à instância temporária, abra o utilitário Disk Management e ative a unidade.
4. Na instância temporária, abra o Regedit e selecione `HKEY_LOCAL_MACHINE`. No menu Arquivo, escolha Carregar Hive. Selecione a unidade, abra o arquivo `Windows\System32\config\SYSTEM` e especifique um nome de chave quando solicitado (você pode usar qualquer nome).
5. Selecione a chave que você acabou de carregar e vá até `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Cada interface de rede é listada por um GUID. Selecione a interface de rede correta. Se o DHCP estiver desabilitado e um endereço IP estático for atribuído, `EnableDHCP` será definido como 0. Para habilitar o DHCP, defina `EnableDHCP` como 1 e exclua as seguintes chaves se existirem: `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Selecione a chave novamente e, no menu Arquivo, escolha Descarregar Hive.

Note

Se você possuir várias interfaces de rede, precisará identificar a interface correta para habilitar o DHCP. Para identificar a interface de rede correta, reveja os seguintes valores de chave `NameServer`, `SubnetMask`, `IPAddress` e `DefaultGateway`. Esses valores exibem a configuração estática da instância anterior.

6. (Opcional) Se o DHCP já estiver ativado, é possível que você não tenha uma rota para o serviço de metadados. Atualizar o EC2Config pode resolver esse problema.

- a. Faça download e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte [Instalar a versão mais recente do EC2Config \(p. 532\)](#).
 - b. Extraia arquivos do arquivo .zip para o diretório Temp na unidade que você associou.
 - c. Abra Regedit e selecione HKEY_LOCAL_MACHINE. No menu Arquivo, escolha Carregar Hive. Selecione a unidade, abra o arquivo Windows\System32\config\SOFTWARE e especifique um nome de chave quando solicitado (você pode usar qualquer nome).
 - d. Selecione a chave que você acabou de carregar e vá até Microsoft\Windows\CurrentVersion. Selecione a chave RunOnce. (Se essa chave não existir, clique com o botão direito do mouse em CurrentVersion, aponte para Novo, selecione Chave e nomeie a chave RunOnce.) Clique com o botão direito do mouse, aponte para Novo e selecione Valor de string. Insira Ec2Install como o nome e C:\Temp\Ec2Install.exe -q como dados.
 - e. Selecione a chave novamente e, no menu Arquivo, escolha Descarregar Hive.
7. (Opcional) Se sua instância temporária for baseada na mesma AMI que a instância original, você deverá concluir as etapas a seguir ou não será possível iniciar a instância original depois de restaurar o volume raiz, por causa de uma colisão de assinatura de disco.

Warning

O procedimento a seguir descreve como editar o Registro do Windows usando o Editor do Registro. Se você não estiver familiarizado com o Registro do Windows ou como fazer alterações com segurança usando o Editor do Registro, consulte[Configure the Registry](#) (Configurar o Registro).

- a. Abra um prompt de comando, digite regedit.exe e pressione Enter.
- b. No Editor do Registro, escolha HKEY_LOCAL_MACHINE no menu contextual (clique com o botão direito do mouse), depois escolha Localizar.
- c. Digite Windows Boot Manager e escolha Localizar Próxima.
- d. Escolha a chave chamada 11000001. Essa chave é irmã da chave que você localizou na etapa anterior.
- e. No painel direito, selecione Element e escolha Modificar no menu de contexto (clique com o botão direito do mouse).
- f. Localize a assinatura de disco de quatro bytes no deslocamento 0x38 nos dados. Inverta os bytes para criar a assinatura de disco e anote-a. Por exemplo, a assinatura de disco representada pelos seguintes dados é E9EB3AA5:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

- g. Em uma janela do prompt de comando, execute o comando a seguir para iniciar o Microsoft DiskPart.

```
diskpart
```

- h. Execute o comando DiskPart a seguir para selecionar o volume. (Você pode verificar se o número do disco é 1 usando o utilitário Gerenciamento de disco.)

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

- i. Execute o comando DiskPart a seguir para obter a assinatura do disco.

```
DISKPART> uniqueid disk  
Disk ID: 0C764FA8
```

- j. Se a assinatura de disco mostrada na etapa anterior não corresponder à assinatura de disco do BCD que você anotou anteriormente, use o seguinte comando DiskPart para alterar a assinatura de disco para que ela corresponda:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. Usando o utilitário Disk Management, desative o volume da unidade.

Note

A unidade ficará offline automaticamente se a instância temporária estiver executando o mesmo sistema operacional que a instância afetada, portanto, você não precisará deixá-la offline manualmente.

9. Desanexe o volume da instância temporária. Você pode encerrar a instância temporária se você não tiver utilização adicional para ela.
10. Restaure o volume raiz da instância afetada anexando o volume como /dev/sda1.
11. Inicie a instância afetada.

Se você estiver conectado à instância, abra um navegador de Internet na instância e insira a seguinte URL do servidor de metadados:

```
http://169.254.169.254/latest/meta-data/
```

Se você não conseguir entrar em contato com o servidor de metadados, tente o seguinte para resolver o problema:

- Faça download e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte [Instalar a versão mais recente do EC2Config \(p. 532\)](#).
- Verifique se a instância Windows está executando drivers PV de RedHat. Em caso afirmativo, atualize os drivers PV. Para obter mais informações, consulte [Atualizar drivers de PV em instâncias do Windows \(p. 565\)](#).
- Verifique se o firewall, o IPSec e as configurações de servidor não bloquearem o tráfego de saída para o serviço de metadados (169.254.169.254) ou os servidores de AWS KMS (os endereços são especificados nos elementos do TargetKMSServer em C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml).
- Verifique se você tem uma rota para o serviço de metadados (169.254.169.254) usando o seguinte comando.

```
route print
```

- Verifique se há problemas de rede que podem afetar a zona de disponibilidade para sua instância. Acesse <http://status.aws.amazon.com/>.

"Não é possível ativar o Windows"

As instâncias do Windows usam a ativação do AWS KMS no Windows. Você pode receber esta mensagem: `A problem occurred when Windows tried to activate. Error Code 0xC004F074`, se sua instância não conseguir acessar o servidor de AWS KMS. O Windows deve ser

ativado a cada 180 dias. O EC2Config tenta entrar em contato com o servidor de AWS KMS antes que o período de ativação expire para garantir que o Windows permaneça ativado.

Se você detectar um problema de ativação do Windows, execute o procedimento a seguir para resolver o problema.

Para EC2Config (AMIs do Windows Server 2012 R2 e anteriores)

1. Faça download e instale a versão mais recente do serviço EC2Config. Para obter mais informações sobre como instalar esse serviço, consulte [Instalar a versão mais recente do EC2Config \(p. 532\)](#).
2. Faça login na instância e abra o seguinte arquivo: C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml.
3. Localize o plugin Ec2WindowsActivate no arquivo config.xml. Altere o estado para Habilitado e salve suas alterações.
4. No snap-in Windows Services, reinicie o serviço EC2Config ou reinicialize a instância.

Se isso não resolver o problema de ativação, siga estas etapas adicionais.

1. Defina o AWS KMS de destino: C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Ative o Windows: C:\> slmgr.vbs /ato

Para EC2Launch (AMIs do Windows Server 2016 e posteriores)

1. De um prompt do PowerShell com direitos administrativos, importe o módulo do EC2Launch:

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Ec2Launch.psd1"
```

2. Chame a função Add-Routes para ver a lista de novas rotas:

```
PS C:\> Add-Routes
```

3. Chamar a função Set-ActivationSettings:

```
PS C:\> Set-Activationsettings
```

4. Em seguida, execute o seguinte script para ativar o Windows:

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Tanto para EC2Config como para EC2Launch, se você ainda estiver recebendo um erro de ativação, verifique as informações a seguir.

- Verifique se você tem rotas para os servidores de AWS KMS. Abra C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml e localize os elementos TargetKMSServer. Execute o comando a seguir e verifique se os endereços para esses servidores de AWS KMS estão listados.

```
route print
```

- Verifique se a chave do cliente de AWS KMS está definida. Execute o seguinte comando e verifique a saída.

```
C:\Windows\System32\slmgr.vbs /dlv
```

Se o resultado contiver o erro Error: product key not found (Erro: chave de produto não encontrada), a chave de cliente do AWS KMS não estará definida. Se a chave de cliente do AWS KMS não estiver definida, procure pela chave de cliente conforme descrito neste artigo da Microsoft: [AWS KMSClient Setup Keys](#) (Chaves de configuração de cliente) e execute o comando a seguir para definir a chave de cliente do AWS KMS.

```
C:\Windows\System32\slmgr.vbs /ipk client_key
```

- Verifique se o sistema tem a hora e o fuso horário corretos. Se você estiver usando o Windows Server 2008 ou posterior e um fuso horário diferente do UTC, adicione a chave de Registro a seguir e defina-a como 1 para garantir que o horário esteja correto: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal.
- Se o Firewall do Windows estiver habilitado, desabilite-o temporariamente usando o seguinte comando.

```
netsh advfirewall set allprofiles state off
```

"O Windows não é genuíno (0x80070005)"

As instâncias do Windows usam a ativação do AWS KMS no Windows. Se uma instância não conseguir concluir o processo de ativação, ela relatará que a cópia do Windows não é genuína.

Tente as sugestões para "Não é possível ativar o Windows" (p. 1642).

"Nenhum servidor de licença do servidor terminal disponível para fornecer uma licença"

Por padrão, o Windows Server é licenciado para dois usuários simultâneos por meio do Remote Desktop. Se você precisar fornecer a mais de dois usuários acesso simultâneo à sua instância Windows por meio do Remote Desktop, compre uma licença de acesso de cliente (CAL) do Remote Desktop Services e instale as funções Remote Desktop Session Host e Remote Desktop Licensing Server.

Verifique se há os seguintes problemas:

- Você excedeu o número máximo de sessões simultâneas de RDP.
- Você instalou a função Windows Remote Desktop Services.
- O licenciamento expirou. Se o licenciamento expirou, você não poderá se conectar à sua instância Windows como um usuário. Você pode tentar o seguinte:
 - Conecte-se à instância da linha de comando usando um parâmetro /admin, por exemplo:

```
mstsc /v:instance /admin
```

Para obter mais informações, consulte o seguinte artigo da Microsoft: [Acessar a área de trabalho remota por meio da linha de comando](#).

- Interrompa a instância, desanexe seus volumes do Amazon EBS e anexe-os a outra instância na mesma zona de disponibilidade para recuperar os dados.

“Algumas configurações são gerenciadas pela sua organização”

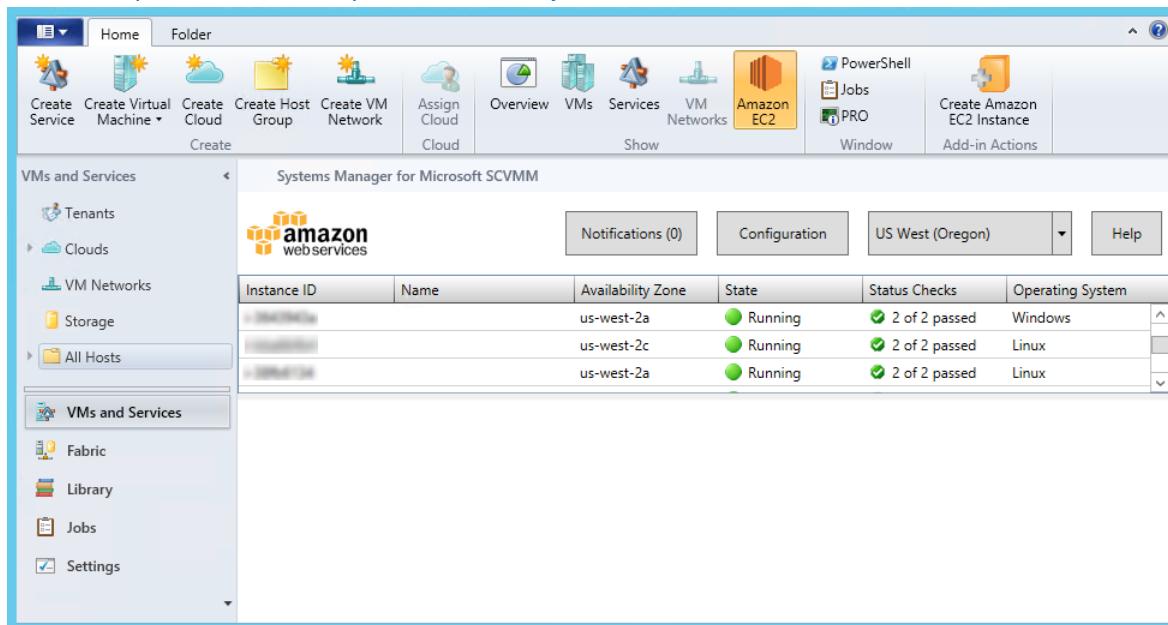
As instâncias executadas a partir das AMIs mais recentes do Windows Server podem exibir uma mensagem do Windows Update informando “Algumas configurações são gerenciadas por sua organização”. Essa mensagem aparece como resultado de alterações no Windows Server e não afeta o comportamento do Windows Update nem sua capacidade de gerenciar as configurações de atualização.

Como remover o aviso

1. Abra gpedit.msc e navegue até Configuração do Computador, Modelos Administrativos, Componentes do Windows, Atualizações do Windows. Edite Configurar a atualização automática e defina-a como habilitada.
2. Em um prompt de comando, atualize a política de grupo usando gpupdate /force.
3. Feche e reabra as configurações do Windows Update. Você verá a mensagem acima sobre as configurações serem gerenciadas por sua organização, seguida por "Baixaremos automaticamente as atualizações, exceto em conexões limitadas (em que taxas podem ser cobradas). Nesse caso, faremos automaticamente download dessas atualizações necessárias para manter o Windows funcionando sem problemas.
4. Retorne para gpedit.msc e defina a política de grupo como não configurada. Execute gpupdate /force novamente.
5. Feche o prompt de comando e aguarde alguns minutos.
6. Reabra as configurações do Windows Update. Você não deve ver a mensagem “Algumas configurações são gerenciadas pela sua organização”

AWS Systems Manager para Microsoft System Center VMM

O AWS Systems Manager para Microsoft System Center Virtual Machine Manager (SCVMM) oferece uma interface simples e fácil de usar para gerenciar os recursos da AWS, como instâncias do EC2, no Microsoft SCVMM. Ele é implementado como um suplemento para o console do VMM. Para obter mais informações, consulte [Suplementos da AWS para o Microsoft System Center](#).



Features

- Os administradores podem conceder permissões para usuários para que eles possam gerenciar instâncias do EC2 no SCVMM.
- Os usuários podem executar, visualizar, reiniciar, interromper, iniciar e encerrar instâncias, se tiverem as permissões necessárias.
- Os usuários podem obter as senhas para suas instâncias do Windows e conectar-se a elas usando RDP.
- Os usuários podem obter nomes DNS públicos para suas instâncias do Linux e conectar-se a elas usando SSH.
- Os usuários podem importar suas máquinas virtuais Hyper-V Windows do SCVMM para o Amazon EC2.

Limitations

- Os usuários devem ter uma conta que eles possam usar para fazer login no SCVMM.
- Você não pode importar máquinas virtuais Linux do SCVMM para o Amazon EC2.

- Essa não é uma ferramenta completa para criar e gerenciar recursos da AWS. O suplemento permite que os usuários do SCVMM comecem a executar tarefas básicas rapidamente para gerenciar suas instâncias do EC2. As futuras versões podem dar suporte ao gerenciamento de recursos adicionais da AWS.

Requirements

- Uma conta da AWS
- Microsoft System Center VMM 2012 R2 ou System Center VMM 2012 SP1 com o pacote cumulativo de atualizações mais recente

Conceitos básicos

Para começar, consulte a seguinte documentação:

- [Configuração \(p. 1647\)](#)
- [Gerenciamento de instâncias do EC2 \(p. 1651\)](#)
- [Solução de problemas \(p. 1658\)](#)

Configurar o AWS Systems Manager para o Microsoft SCVMM

Quando você configura o AWS Systems Manager, os usuários em sua organização poderão acessar os recursos da AWS. O processo envolve a criação de contas, a implantação do suplemento e o fornecimento de suas credenciais.

Tarefas

- [Cadastre-se no AWS \(p. 1647\)](#)
- [Configurar o acesso para usuários \(p. 1648\)](#)
- [Implantar o suplemento \(p. 1650\)](#)
- [Forneça suas credenciais da AWS \(p. 1650\)](#)

Cadastre-se no AWS

Quando você se cadastra na Amazon Web Services, a conta da AWS é cadastrada automaticamente em todos os serviços da AWS. Você será cobrado apenas pelos serviços que usar.

Se já tiver uma conta da AWS, passe para a próxima tarefa. Se você ainda não possuir uma conta da AWS, use o procedimento a seguir para criar uma.

Para se cadastrar em uma conta da AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga as instruções online.

Parte do procedimento de cadastro envolve uma chamada telefônica e a digitação de um código de verificação usando o teclado do telefone.

Configurar o acesso para usuários

A primeira vez que você usar o Systems Manager, forneça as credenciais da AWS. Para permitir que vários usuários acessem a mesma conta da AWS usando credenciais e permissões exclusivas, crie um usuário do IAM para cada usuário. Você pode criar um ou mais grupos com políticas que concedam permissões para executar tarefas limitadas. Em seguida, é possível criar um ou mais usuários do IAM e adicionar cada usuário ao grupo apropriado.

Para criar um grupo de administradores

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Groups e escolha, Create New Group.
3. Na caixa Nome do grupo, especifique **Administrators** e, em seguida, escolha Próxima etapa.
4. Na página Attach Policy (Anexar política), selecione a política AdministratorAccess gerenciada pela AWS.
5. Selecione Next Step (Próxima etapa) e, em seguida, Create Group (Criar grupo).

Para criar um grupo com acesso limitado ao Amazon EC2

1. Abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação, escolha Groups e escolha, Create New Group.
3. Na caixa Nome do grupo, especifique um nome significativo para o grupo e, em seguida, escolha Próxima etapa.
4. Na página Attach Policy (Anexar política), não selecione uma política gerenciada pela AWS. Escolha Next Step (Próxima etapa) e Create Group (Criar grupo).
5. Escolha o nome do grupo que você acabou de criar. Na guia Permissões, escolha Políticas em linha e, em seguida, clique aqui.
6. Selecione o botão Política personalizada e, então, Selecionar.
7. Digite um nome para a política e um documento de política que conceda acesso limitado ao Amazon EC2 e, em seguida, selecione Aplicar política. Por exemplo, você pode especificar uma das políticas personalizadas a seguir.

Conceda aos usuários nesse grupo permissão somente para visualizar informações sobre instâncias do EC2

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:Describe*",  
                "iam>ListInstanceProfiles"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Conceda aos usuários nesse grupo permissão para executar todas as operações nas instâncias do EC2 às quais o suplemento oferece suporte

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {
```

```
{  
    "Effect": "Allow",  
    "Action": [  
        "iam:ListInstanceProfiles", "iam:PassRole",  
        "ec2:Describe*", "ec2>CreateKeyPair",  
        "ec2>CreateTags", "ec2>DeleteTags",  
        "ec2:RunInstances", "ec2:GetPasswordData",  
        "ec2:RebootInstances", "ec2:StartInstances",  
        "ec2:StopInstances", "ec2:TerminateInstances"  
    ],  
    "Resource": "*"  
}  
}  
}
```

Conceda aos usuários nesse grupo permissão para importar uma VM para o Amazon EC2

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "s3>ListAllMyBuckets", "s3>CreateBucket",  
                "s3>DeleteBucket", "s3>DeleteObject",  
                "s3:GetBucketLocation", "s3GetObject",  
                "s3>ListBucket", "s3PutObject",  
                "ec2:DescribeTags", "ec2:CancelConversionTask",  
                "ec2:DescribeConversionTasks", "ec2:DescribeInstanceAttribute",  
                "ec2>CreateImage", "ec2:AttachVolume",  
                "ec2:ImportInstance", "ec2:ImportVolume",  
                "dynamodb:DescribeTable", "dynamodb CreateTable",  
                "dynamodb:Scan", "dynamodb:PutItem", "dynamodb:UpdateItem"  
            ],  
            "Resource": "*"  
        }  
    ]  
}
```

Para criar um usuário do IAM, obtenha as credenciais do usuário da AWS e conceda permissões ao usuário

1. No painel de navegação, escolha Usuários e depois Adicionar usuário.
2. Digite um nome de usuário.
3. Selecione o tipo de acesso que este conjunto de usuários terá. Selecione Programmatic access (Acesso programático) e AWS Management Console access (Acesso ao console) se este usuário também deve acessar o AWS Management Console.
4. Em Tipo de senha do console, selecione uma das opções abaixo:
 - Autogenerated password. Cada usuário obtém uma senha gerada de forma aleatória que atenda à política de senha atual em vigor (se houver). Você pode visualizar ou fazer download das senhas ao acessar a página Final.
 - Custom password. A cada usuário é atribuída a senha digitada na caixa.
5. Escolha Próximo: Permissões .
6. Na página Definir permissões, escolha Adicionar usuário ao grupo. Selecione o grupo apropriado.
7. Escolha Próximo: Revisão e, em seguida, Criar usuário.
8. Para visualizar as chaves de acesso dos usuários (IDs de chave de acesso e chaves de acesso secretas), escolha Mostrar ao lado de cada senha e chave de acesso secreta que você deseja ver.

Para salvar as chaves de acesso, escolha Fazer download de .csv e, em seguida, salve o arquivo em um local seguro.

Note

Não é possível recuperar a chave de acesso secreta depois de concluir essa etapa. Se você a perder, deverá criar uma nova.

9. Escolha Close (Fechar).

Implantar o suplemento

Os suplementos do System Center VMM são distribuídos com arquivos .zip. Para implantar o suplemento, use o procedimento a seguir.

Para implantar o suplemento

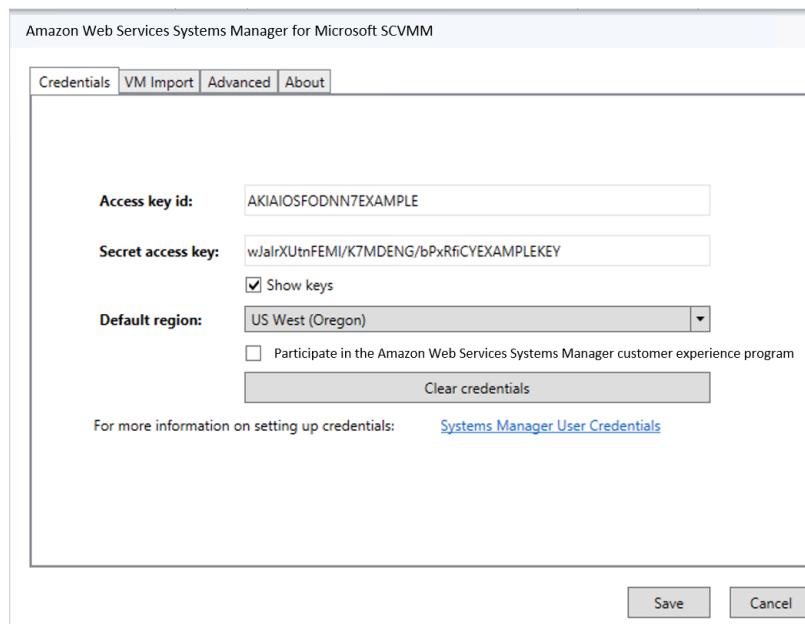
1. Na sua instância, acesse o [AWS Systems Manager para Microsoft System Center Virtual Machine Manager](#) e clique em SCVMM. Salve o arquivo aws-systems-manager-1.5.zip em sua instância.
2. Abra o console do VMM.
3. No painel de navegação, clique em Configurações e em Suplementos do console.
4. Na fita, clique em Importar suplemento do console.
5. Na página Selecionar suplemento, clique em Procurar e selecione o arquivo aws-systems-manager-1.5.zip do suplemento que você baixou.
6. Ignore todos os avisos de que há conjuntos no suplemento que não estão assinados por uma autoridade confiável. Selecione Continuar a instalar este suplemento em clique em Avançar.
7. Na página Resumo, clique em Concluir.
8. Quando o suplemento for importado, o status do trabalho será Completed. Você pode fechar a janela Trabalhos.

Forneça suas credenciais da AWS

Ao usar o Systems Manager pela primeira vez, você deverá fornecer as credenciais da AWS. Suas chaves de acesso identificam você para a AWS. Há dois tipos de chaves de acesso: IDs de chave de acesso (por exemplo, AKIAIOSFODNN7EXAMPLE) e chaves de acesso secretas (por exemplo, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Você deve ter armazenado suas chaves de acesso em um lugar seguro quando as recebeu.

Forneça suas credenciais da AWS.

1. Abra o console do VMM.
2. No painel de navegação, clique em VMs e serviços.
3. Na fita, clique em Amazon EC2.
4. Na guia Credentials (Credenciais), especifique suas credenciais da AWS, selecione uma região padrão e clique em Save (Salvar).



Para alterar essas credenciais a qualquer momento, clique em Configuração.

Gerenciar instâncias do EC2 usando o AWS Systems Manager para Microsoft SCVMM

Depois de fazer login no console do Systems Manager usando suas credenciais da AWS, você pode gerenciar as instâncias do EC2.

Tarefas

- [Criar uma instância do EC2 \(p. 1651\)](#)
- [Visualizar suas instâncias \(p. 1654\)](#)
- [Conecte-se à sua instância \(p. 1654\)](#)
- [Reinicializar a instância \(p. 1655\)](#)
- [Parar a instância \(p. 1655\)](#)
- [Executar sua instância. \(p. 1655\)](#)
- [Encerrar a instância \(p. 1655\)](#)

Criar uma instância do EC2

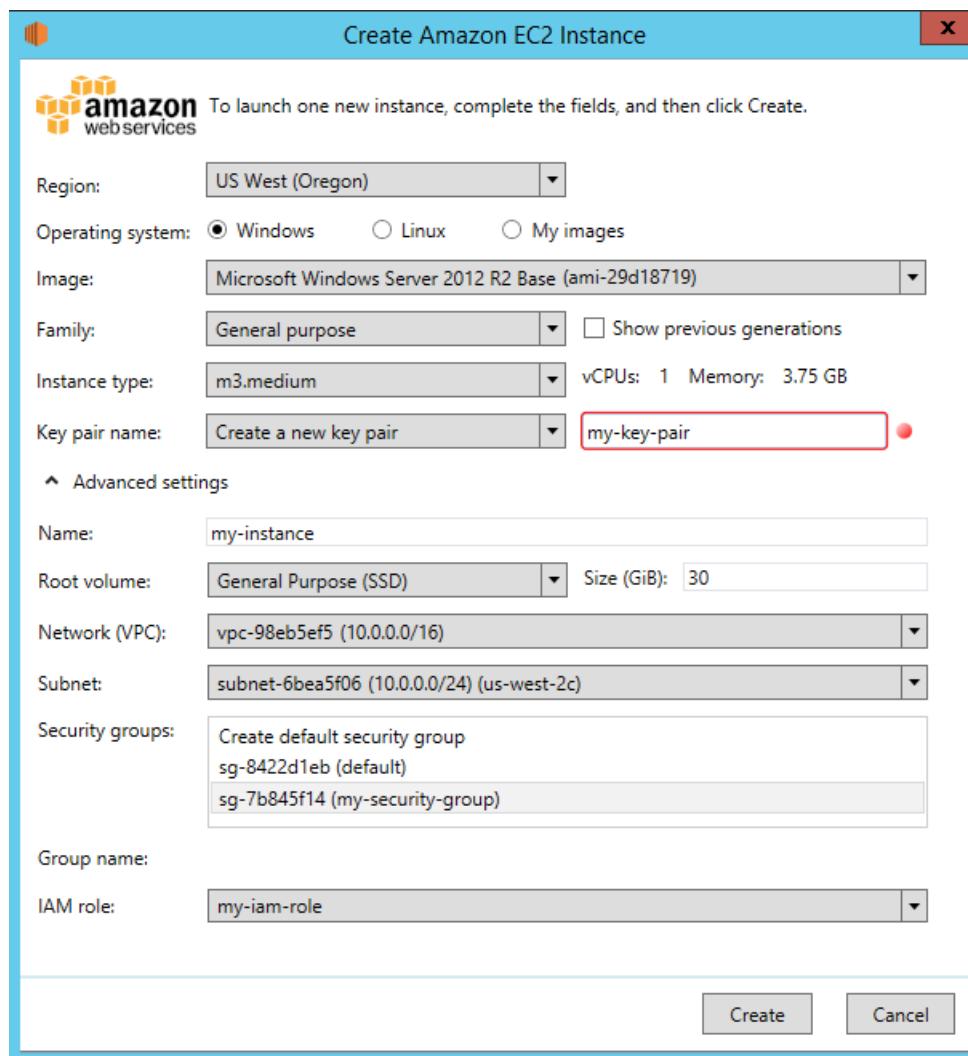
As permissões que você recebeu do administrador determinam se você pode ou não criar instâncias.

Prerequisites

- Uma nuvem privada virtual (VPC) com uma sub-rede na zona de disponibilidade na qual você executará a instância. Para obter mais informações sobre como criar uma VPC, consulte o [Guia de conceitos básicos da Amazon VPC](#).

Para criar uma instância do EC2

1. Abra o SCVMM.
2. Na fita, clique em Criar instância do Amazon EC2.
3. Preencha a caixa de diálogo Criar instância do Amazon EC2 da seguinte forma:
 - a. Selecione uma região para sua instância. Por padrão, selecionamos a região que você configurou como sua região padrão.
 - b. Selecione um modelo (conhecido como AMI) para sua instância. Para usar AMIs fornecidas pela Amazon, selecione Windows ou Linux e, em seguida, selecione uma AMI em Imagem. Para usar AMIs que você criou, selecione Minhas imagens e escolha uma AMI em Imagem.
 - c. Selecione o tipo da instância. Primeiro, selecione uma das famílias de instâncias mais recentes em Família e escolha um tipo de instância em Tipo de instância. Para incluir famílias de instâncias da geração anterior na lista, selecione Mostrar gerações anteriores. Para obter mais informações, consulte [Instâncias do Amazon EC2](#) e [Instâncias de gerações anteriores](#).
 - d. Crie ou selecione um par de chaves. Para criar um par de chaves, selecione `Create a new key pair` em Nome do par de chaves e digite um nome para o par de chaves no campo realçado (por exemplo, `my-key-pair`).
 - e. (Opcional) Em Configurações avançadas, especifique um nome de exibição para a instância.
 - f. (Opcional) Em Configurações avançadas, selecione uma VPC em Rede (VPC). Essa lista inclui todas as VPCs para a região, incluindo as VPCs criadas usando o console de Amazon VPC e a VPC padrão (se existir). Caso você tenha uma VPC padrão nessa região, a selecionaremos por padrão. Se o texto for "There is no VPC available for launch or import operations in this region" (Não há VPC disponível para operações de execução ou importação nessa região), você deverá criar uma VPC nessa região usando o console da Amazon VPC.
 - g. (Opcional) Em Configurações avançadas, selecione uma sub-rede em Sub-rede. Essa lista inclui todas as sub-redes para a VPC selecionada, incluindo todas as sub-redes padrão. Se essa lista estiver vazia, você deverá adicionar uma sub-rede à VPC usando o console de Amazon VPC ou selecionar outra VPC. Caso contrário, selecionaremos uma sub-rede para você.
 - h. (Opcional) Em Configurações avançadas, crie um security group ou selecione um ou mais security groups. Se você selecionar `Create default security group`, criaremos um grupo de segurança que concederá acesso RDP e SSH a todos, o que você pode modificar usando o console do Amazon EC2 ou de Amazon VPC. Você pode digitar um nome para esse security group na caixa Nome do grupo.
 - i. (Opcional) Em Configurações avançadas, selecione uma função do IAM. Se essa lista estiver vazia, você poderá criar uma função usando o console do IAM.



4. Clique em Criar. Se você estiver criando um par de chaves, será solicitado a salvar o arquivo .pem. Salve esse arquivo em um lugar seguro; você precisará dele para fazer login em sua instância. Você receberá a confirmação de que a instância foi executada. Clique em Close.

Depois de criar sua instância, ela aparecerá na lista de instâncias para a região na qual você a executou. Inicialmente, o status da instância é pending. Depois que o status mudar para running, a instância estará pronta para uso.

Você pode controlar o ciclo de vida de sua instância usando o Systems Manager, como descrito nesta página. Para executar outras tarefas, como a seguinte, você deve usar o AWS Management Console:

- Anexar um volume do Amazon EBS à instância (p. 1271)
- Associar um endereço IP elástico à instância (p. 997)
- Habilitar a proteção contra encerramento (p. 476)

Visualizar suas instâncias

As permissões que o administrador conceder a você determinarão se você visualizará instâncias e obterá informações detalhadas sobre elas.

Para visualizar suas instâncias e obter informações detalhadas

1. Abra o [console do AWS Systems Manager](#).
2. Selecione uma região na lista de regiões.
3. Na lista de instâncias, selecione uma ou mais instâncias.
4. No painel inferior, clique na seta para baixo ao lado de cada instância para visualizar informações detalhadas sobre a instância.

^ [i-343e9f3a \(my-instance\)](#)

Virtual machine information		Networking
Instance ID:	i-343e9f3a	Public DNS name:
Name:	my-instance	Public IP address:
State:	Running	Private DNS name:
Launch time:	1/20/2015 12:26:48 PM -08:00 (1 minute ago)	ip-10-0-0-147.us-west-2.compute.internal
Instance type:	m3.medium	Private IP address:
Tenancy:	default	Vpc ID:
Image ID:	ami-29d18719	Subnet ID:
Operating system:	Windows	Network interfaces:

Conecte-se à sua instância

Você pode fazer login em uma instância do EC2 se tiver a chave privada (arquivo `.pem`) para o par de chaves que foi especificado para execução da instância. A ferramenta que você usará para se conectar à sua instância depende de se a instância é Windows ou Linux.

Para se conectar a uma instância do EC2 do Windows

1. Aberto AWS Systems Manager.
2. Na lista de instâncias, selecione a instância, clique com o botão direito do mouse e, em seguida, clique em Recuperar senha do Windows.
3. Na caixa de diálogo Recuperar senha padrão do administrador do Windows, clique em Procurar. Selecione o arquivo de chave privada para o par de chaves e clique em Abrir.
4. Clique em Decrypt Password. Salve a senha ou copie-a na área de transferência.
5. Selecione a instância, clique com o botão direito do mouse e clique em Conectar via RDP. Quando as credenciais forem solicitadas, use o nome da conta de administrador e a senha que você salvou na etapa anterior.
6. Como o certificado está autoassinado, é possível que você receba um aviso de que o certificado de segurança não é de uma autoridade de certificação confiável. Clique em Sim para continuar.

Se a conexão falhar, consulte [Solução de problemas em instâncias Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Para se conectar a uma instância do EC2 do Linux

1. Aberto AWS Systems Manager.
2. Na lista de instâncias, selecione a instância.

3. No painel inferior, clique na seta para baixo ao lado do ID da instância para visualizar informações detalhadas sobre a instância.
4. Localize o nome DNS público. Você precisará dessas informações para se conectar à sua instância.
5. Conecte-se à instância usando PuTTY. Para obter instruções passo a passo, consulte [Conectar-se à sua instância do Linux a partir do Windows usando o PuTTY](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

Reiniciar a instância

As permissões que você recebeu do administrador determinam se você pode ou não reiniciar instâncias.

Para reiniciar sua instância

1. Aberto AWS Systems Manager.
2. Na lista de instâncias, selecione a instância.
3. Clique com o botão direito na instância e clique em Redefinir (Reiniciar).
4. Quando a confirmação for solicitada, clique em Yes.

Parar a instância

As permissões que você recebeu do administrador determinam se você pode ou não interromper instâncias.

Para interromper a instância

1. Aberto AWS Systems Manager.
2. Na lista de instâncias, selecione a instância.
3. Clique com o botão direito na instância e clique em Desligar (Interromper).
4. Quando a confirmação for solicitada, clique em Yes.

Executar sua instância.

As permissões que você recebeu do administrador determinam se você pode ou não iniciar instâncias.

Para iniciar a instância

1. Aberto AWS Systems Manager.
2. Na lista de instâncias, selecione a instância.
3. Clique com o botão direito na instância e clique em Ligar (Iniciar).
4. Quando a confirmação for solicitada, clique em Yes.

Se você obtiver um erro de cota ao tentar iniciar uma instância, você atingiu o limite de instâncias em execução simultânea. O limite padrão para sua conta da AWS é 20. Se você precisar de instâncias em execução adicionais, preencha o formulário em [Solicitação para aumentar o limite de instâncias do Amazon EC2](#).

Encerrar a instância

As permissões que você recebeu do administrador determinam se você pode ou não encerrar instâncias.

Para encerrar sua instância

1. Aberto AWS Systems Manager.
2. Na lista de instâncias, selecione a instância.
3. Clique com o botão direito do mouse na instância e clique em Excluir (Encerrar).
4. Quando a confirmação for solicitada, clique em Yes.

Importar sua máquina virtual usando o AWS Systems Manager para Microsoft SCVMM

Você pode executar uma instância do EC2 de uma máquina virtual que você importar do SCVMM para o Amazon EC2.

Important

Você não pode importar máquinas virtuais Linux do SCVMM para o Amazon EC2.

Tópicos

- [Prerequisites \(p. 1656\)](#)
- [Importar sua máquina virtual \(p. 1656\)](#)
- [Verificar o status da tarefa de importação \(p. 1657\)](#)
- [Fazer backup de sua instância importada \(p. 1658\)](#)

Prerequisites

- Certifique-se de que a VM esteja pronta. Para obter mais informações, consulte [Preparar sua VM](#) no Guia do usuário de VM Import/Export.
- No AWS Systems Manager, clique em Configuration (Configuração), selecione a guia VM Import (Importação da VM) e revise as seguintes configurações:
 - Prefixo do bucket do S3: criamos um bucket para que seja feito o upload de imagens de disco antes de serem importadas. O nome do bucket começa com o prefixo indicado aqui e inclui a região (por exemplo, us-east-2). Para excluir as imagens de disco depois de serem importadas, selecione Limpar o bucket do S3 após a importação.
 - Caminho de exportação de imagens de VM: um local para as imagens de disco exportadas da VM. Para excluir as imagens de disco depois de serem importadas, selecione Limpar o caminho de exportação após a importação.
 - Alternar caminho do módulo do Hyper-V PowerShell: o local do módulo do Hyper-V PowerShell, se não estiver instalado no local padrão. Para obter mais informações, consulte [Instalação de ferramentas de gerenciamento do Hyper-V](#) na Biblioteca TechNet da Microsoft.

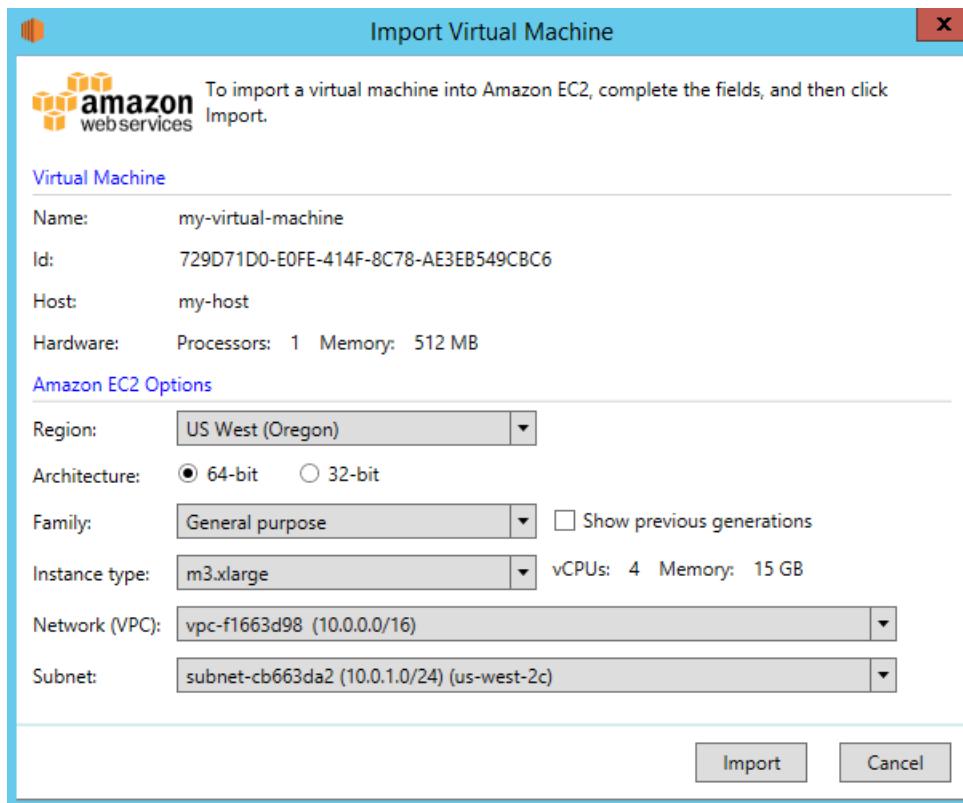
Importar sua máquina virtual

As permissões que você tiver recebido do administrador determinam se você pode importar máquinas virtuais HyperV Windows do SCVMM para a AWS.

Para importar sua máquina virtual

1. Abra o SCVMM.
2. Na fita, clique em VMs. Selecione a máquina virtual na lista.
3. Na fita, clique em Importar VM para o Amazon EC2.

4. Preencha a caixa de diálogo Importar máquina virtual da seguinte forma:
 - a. Selecione uma região para a instância. Por padrão, selecionamos a região que você configurou como sua região padrão.
 - b. Selecione o tipo da instância. Primeiro, selecione uma das famílias de instâncias mais recentes em Família e escolha um tipo de instância em Tipo de instância. Para incluir famílias de instâncias da geração anterior na lista, selecione Mostrar gerações anteriores. Para obter mais informações, consulte [Instâncias do Amazon EC2](#) e [Instâncias de gerações anteriores](#).
 - c. Selecione uma VPC em Rede (VPC). Essa lista inclui todas as VPCs para a região, incluindo as VPCs criadas usando o console de Amazon VPC e a VPC padrão (se existir). Caso você tenha uma VPC padrão nessa região, a selecionaremos por padrão. Se o texto for "Não há VPC disponível para operações de execução ou importação nessa região", você deve criar uma VPC nessa região usando o console da Amazon VPC.
 - d. Selecione uma sub-rede em Sub-rede. Essa lista inclui todas as sub-redes para a VPC selecionada, incluindo todas as sub-redes padrão. Se essa lista estiver vazia, você deverá adicionar uma sub-rede à VPC usando o console de Amazon VPC ou selecionar outra VPC. Caso contrário, selecionaremos uma sub-rede para você.



5. Clique em Importar. Se você não tiver especificado as informações necessárias na guia VM Import, você receberá um erro solicitando as informações necessárias. Caso contrário, você receberá a confirmação de que a tarefa de importação foi iniciada. Clique em Close.

Verificar o status da tarefa de importação

A tarefa de importação pode levar algumas horas para ser concluída. Para exibir o status atual, abra o AWS Systems Manager e clique em Notifications (Notificações).

Você receberá as seguintes notificações durante a tarefa de importação:

- Import VM: Created Import VM Task
- Import VM: Export VM Disk Image Done
- Import VM: Upload to S3
- Import VM: Image Conversion Starting
- Import VM: Image Conversion Done
- Import VM: Import Complete

Você receberá as notificações Import VM: Upload to S3, Import VM: Image Conversion Starting e Import VM: Image Conversion Done para cada imagem de disco convertida.

Se houver falha na tarefa de importação, você receberá a notificação Import VM: Import Failed. Para obter mais informações sobre como solucionar problemas com tarefas de importação, consulte [Erros ao importar uma máquina virtual \(p. 1659\)](#).

Fazer backup de sua instância importada

Após o término da operação de importação, a instância é executada até que ela seja encerrada. Se sua instância for concluída, você não poderá se conectar nem recuperar a instância. Se necessário, para garantir que você possa iniciar uma nova instância com o mesmo software que uma instância importada, crie uma Imagem de máquina da Amazon (AMI) de instância importada. Para obter mais informações, consulte [Criar uma AMI do Windows personalizada \(p. 39\)](#).

Solução de problemas do AWS Systems Manager para Microsoft SCVMM

Veja a seguir erros comuns e etapas de solução de problemas.

Tópicos

- [Erro: Não é possível instalar o suplemento \(p. 1658\)](#)
- [Erros de instalação \(p. 1659\)](#)
- [Verificar o arquivo de log \(p. 1659\)](#)
- [Erros ao importar uma máquina virtual \(p. 1659\)](#)
- [Desinstalar o suplemento \(p. 1660\)](#)

Erro: Não é possível instalar o suplemento

Se você receber o seguinte erro, tente instalar o [KB2918659](#) no computador executando o console do VMM. Para obter mais informações, consulte [Descrição do pacote cumulativo de atualizações 5 do System Center 2012 SP1](#). Você não precisará instalar todas as atualizações indicadas neste documento para resolver esse problema, apenas o KB2918659.

```
Add-in cannot be installed
The assembly "Amazon.Scvmm.Addin" referenced to by add-in component "AWS Systems Manager
for
Microsoft SCVMM" could not be found in the add-in package. This could be due to the
following
reasons:
1. The assembly was not included with the add-in package.
```

- 2. The AssemblyName attribute for the add-in does not match the name of the add-in assembly.
- 3. The assembly file is corrupt and cannot be loaded.

Erros de instalação

Se você receber um dos seguintes erros durante a instalação, provavelmente é devido a um problema com o SCVMM:

Could not update managed code add-in pipeline due to the following error:
Access to the path 'C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager \Bin\AddInPipeline\PipelineSegments.store' is denied.

Could not update managed code add-in pipeline due to the following error:
The required folder 'C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager \Bin\AddInPipeline\HostSideAdapters' does not exist.

Add-in cannot be installed
The assembly "Microsoft.SystemCenter.VirtualMachineManager.UIAddIns.dll" referenced by the add-in assembly "Amazon.Scvmm.AddIn" could not be found in the add-in package. Make sure that this assembly was included with the add-in package.

Tente uma das seguintes etapas para contornar esse problema:

- Conceda aos usuários autenticados permissão para ler e executar a pasta C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\Bin\AddInPipeline. No Windows Explorer, clique com o botão direito do mouse na pasta, selecione Propriedades e a guia Segurança.
- Feche o console do SCVMM e inicie-o uma vez como um administrador. No menu Iniciar, localize o SCVMM, clique com o botão direito do mouse e selecione Executar como administrador.

Verificar o arquivo de log

Se você tiver um problema ao usar o suplemento, verifique o arquivo de log gerado, %APPDATA%\Amazon\SCVMM\ec2addin.log, para obter informações úteis.

Erros ao importar uma máquina virtual

O arquivo de log %APPDATA%\Amazon\SCVMM\ec2addin.log, contém informações detalhadas sobre o status de uma tarefa de importação. Veja a seguir erros comuns que você pode ver no arquivo de log ao importar sua VM do SCVMM para o Amazon EC2.

Erro: Não é possível extrair o objeto VirtualMachine do Hyper-V

Solução: Configure o caminho para o módulo Hyper-V PowerShell.

Erro: Você não tem permissão para executar a operação

Esse erro normalmente ocorre quando o Hyper-V não pode salvar a imagem de VM no caminho configurado. Para resolver esse problema, faça o seguinte.

1. Crie um diretório no servidor do Hyper-V. Por exemplo: C:\vmimages.
2. Compartilhe o diretório recém-criado no Hyper-V. Qualquer usuário que execute o SCVMM deve ter acesso ao diretório.

3. No plug-in, defina o caminho de exportação para \\hyperv\vmimages.
4. Execute a exportação.

A imagem será exportada para um diretório local no servidor do Hyper-V. O plug-in do SCVMM o extrairá do Hyper-V e o carregará no Amazon S3.

Desinstalar o suplemento

Se você precisar desinstalar o suplemento, use o procedimento a seguir.

Para desinstalar o suplemento

1. Abra o console do VMM.
2. Selecione o workspace Configurações e clique em Suplementos do console.
3. Select AWS Systems Manager for Microsoft SCVMM.
4. Na fita, clique em Remover.
5. Quando a confirmação for solicitada, clique em Yes.

Se você reinstalar o suplemento depois de desinstalá-lo e receber o erro a seguir, exclua o caminho como sugerido pela mensagem de erro.

```
Error (27301)
There was an error while installing the add-in. Please ensure that the following path does
not
exist and then try the installation again.

C:\Program Files\Microsoft System Center 2012\Virtual Machine Manager\Bin\AddInPipeline\
AddIns\EC2WINDOWS...
```

AWS Management Pack for Microsoft System Center

A AWS oferece um conjunto completo de serviços de aplicações e infraestrutura para execução de quase qualquer coisa na nuvem, desde aplicações empresariais e projetos de big data a jogos sociais e aplicativos móveis. O AWS Management Pack for Microsoft System Center fornece disponibilidade e recursos de monitoramento de performance para as aplicações executadas na AWS.

O AWS Management Pack permite que o Microsoft System Center Operations Manager acesse os recursos da AWS (como instâncias e volumes), para que possa coletar dados de performance e monitorar os recursos da AWS. O AWS Management Pack é uma extensão ao System Center Operations Manager. Há duas versões do AWS Management Pack: uma para o System Center 2012 — Operations Manager e outra para o System Center Operations Manager 2007 R2.

O AWS Management Pack usa métricas e alarmes do Amazon CloudWatch para monitorar seus recursos da AWS. As métricas do Amazon CloudWatch são exibidas no Microsoft System Center como contadores de performance e os alarmes do Amazon CloudWatch são exibidos como alertas.

Você pode monitorar os seguintes recursos:

- Instâncias do EC2
- Volumes do EC2
- Load balancers ELB
- Grupos e zonas de disponibilidade do Amazon EC2 Auto Scaling
- Aplicativos Elastic Beanstalk
- Pilhas do CloudFormation
- Alarmes do CloudWatch
- Métricas personalizadas do CloudWatch

Tópicos

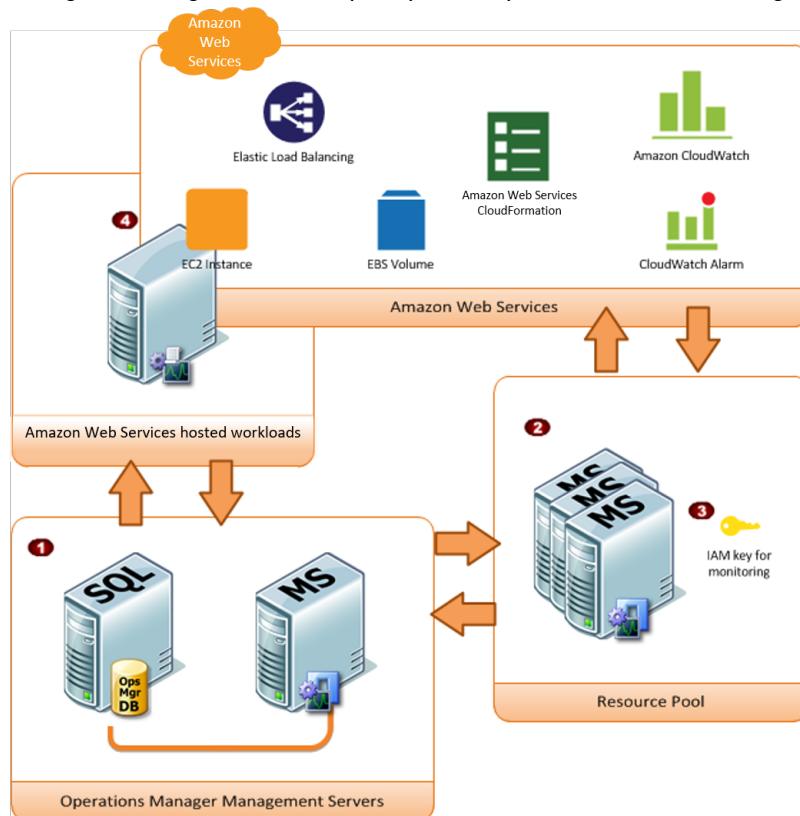
- [Visão geral do AWS Management Pack para o System Center 2012 \(p. 1661\)](#)
- [Visão geral do AWS Management Pack para o System Center 2007 R2 \(p. 1663\)](#)
- [Fazer download do AWS Management Pack \(p. 1664\)](#)
- [Implantar o AWS Management Pack \(p. 1665\)](#)
- [Usar o AWS Management Pack \(p. 1676\)](#)
- [Atualizar o AWS Management Pack \(p. 1697\)](#)
- [Desinstalar o AWS Management Pack \(p. 1698\)](#)
- [Solucionar problemas do AWS Management Pack \(p. 1698\)](#)

Visão geral do AWS Management Pack para o System Center 2012

O AWS Management Pack para System Center 2012 — Operations Manager usa um grupo de recursos que contém um ou mais servidores de gerenciamento para descobrir e monitorar os recursos da AWS.

Você pode adicionar servidores de gerenciamento ao grupo conforme aumenta o número de recursos da AWS que você usa.

O diagrama a seguir mostra os principais componentes do AWS Management Pack.



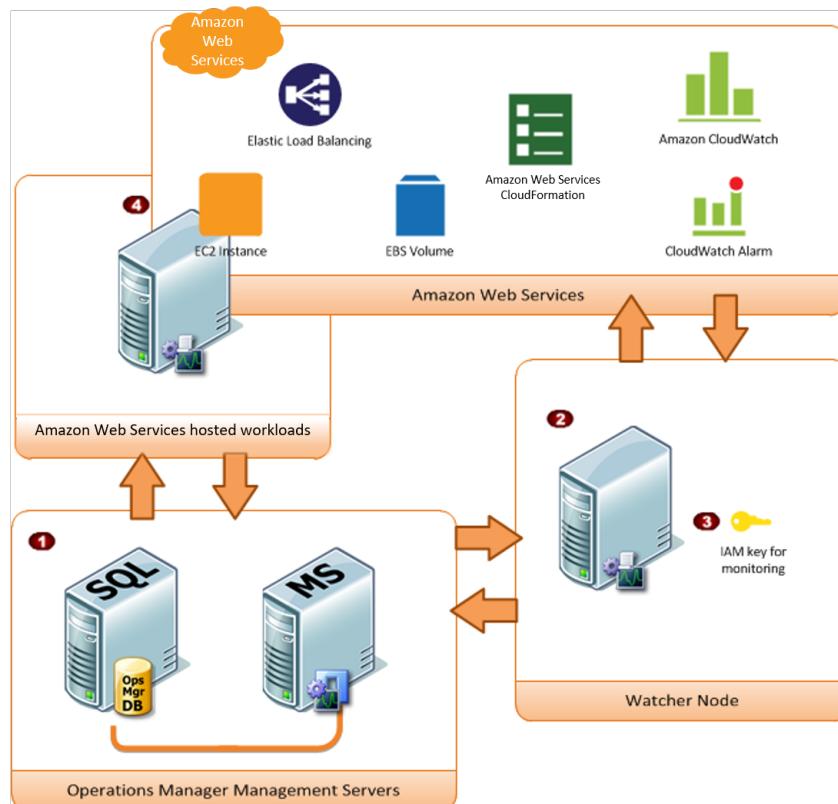
Item	Componente	Descrição
1	Infraestrutura do Operations Manager	Um ou mais servidores de gerenciamento e suas dependências, como o Microsoft SQL Server e um domínio do Microsoft Active Directory. Esses servidores podem ser implantados no local ou na Nuvem AWS. Há suporte para os dois cenários.
2	Grupo de recursos	Um ou mais servidores de gerenciamento usados para comunicação com a AWS usando o AWS SDK para .NET. Esses servidores devem ter conectividade com a Internet.
3	AWSCredenciais da	Um ID da chave de acesso e uma chave de acesso secreta usados pelos servidores de gerenciamento para fazer chamadas de API da AWS. Você deve especificar essas credenciais ao configurar o AWS Management Pack. Recomendamos que você crie um usuário do IAM com privilégios de somente leitura e use essas credenciais. Para obter mais informações sobre como criar um usuário do IAM, consulte Adding a New User to Your AWS Account (Como adicionar um novo usuário à sua conta da AWS) , no IAM User Guide (Guia do usuário do IAM).
4	Instâncias do EC2	Computadores virtuais executados na Nuvem AWS. Algumas instâncias podem ter o Operations Manager Agent instalado,

Item	Componente	Descrição
		enquanto outras talvez não tenham. Quando você instala o Operations Manager Agent, você pode ver a integridade do sistema operacional e dos aplicativos separadamente da integridade da instância.

Visão geral do AWS Management Pack para o System Center 2007 R2

O AWS Management Pack para System Center Operations Manager 2007 R2 usa um computador designado que se conecta ao ambiente do System Center e tem acesso à Internet, chamado de nó observador, para chamar APIs da AWS para descobrir e coletar remotamente informações sobre os recursos da AWS.

O diagrama a seguir mostra os principais componentes do AWS Management Pack.



Item	Componente	Descrição
①	Infraestrutura do Operations Manager	Um ou mais servidores de gerenciamento e suas dependências, como o Microsoft SQL Server e um domínio do Microsoft Active Directory. Esses servidores podem ser implantados no local ou na Nuvem AWS. Há suporte para os dois cenários.
②	Nó observador	Um computador designado gerenciado por agente usado para comunicação com a AWS usando o AWS SDK para .NET.

Item	Componente	Descrição
		Ele pode ser implantado no local ou na Nuvem AWS, mas deve ser um computador gerenciado por agente e deve ter conectividade com a Internet. Você pode usar exatamente um nó observador para monitorar uma conta da AWS. No entanto, um nó observador não pode monitorar várias contas da AWS. Para obter mais informações sobre como configurar um nó observador, consulte Como implantar agentes do Windows na documentação do Microsoft System Center.
3	AWSCredenciais da	Um ID da chave de acesso e uma chave de acesso secreta usados pelo nó observador para fazer chamadas de API da AWS. Você deve especificar essas credenciais ao configurar o AWS Management Pack. Recomendamos que você crie um usuário do IAM com privilégios de somente leitura e use essas credenciais. Para obter mais informações sobre como criar um usuário do IAM, consulte Adding a New User to Your AWS Account (Como adicionar um novo usuário à sua conta da AWS) , no IAM User Guide (Guia do usuário do IAM).
4	Instâncias do EC2	Computadores virtuais executados na Nuvem AWS. Algumas instâncias podem ter o Operations Manager Agent instalado, enquanto outras talvez não tenham. Quando você instala o Operations Manager Agent, você pode ver a integridade do sistema operacional e dos aplicativos separadamente da integridade da instância.

Fazer download do AWS Management Pack

Para começar, faça download do AWS Management Pack. O AWS Management Pack é gratuito. Você pode ser cobrado pelo Amazon CloudWatch, dependendo de como você configura o monitoramento ou de quantos recursos da AWS você monitora.

System Center 2012

Antes de fazer download do AWS Management Pack, verifique se seus sistemas atendem aos seguintes requisitos e pré-requisitos do sistema.

Requisitos do sistema

- System Center Operations Manager 2012 R2 ou System Center Operations Manager 2012 SP1
- Atualização cumulativa 1 ou posterior. Você deve implantar a atualização nos servidores de gerenciamento que monitoram os recursos da AWS, bem como os agentes que executam os nós observadores e os agentes a serem monitorados pelo AWS Management Pack. Recomendamos implantar as atualizações mais recentes disponíveis do Operations Manager em todos os computadores que monitoram os recursos da AWS.
- Microsoft.Unix.Library MP versão 7.3.2026.0 ou posterior

Prerequisites

- Seu datacenter deve ter pelo menos um servidor de gerenciamento configurado com conectividade com a Internet. Os servidores de gerenciamento devem ter a versão 4.5 do Microsoft .NET Framework ou posterior e o PowerShell 2.0 ou posterior instalados.

- A conta de ação do servidor de gerenciamento deve ter privilégios de administrador local no servidor de gerenciamento.

Para fazer download do AWS Management Pack

1. No site [Suplementos da AWS para o Microsoft System Center](#), clique em SCOM 2012.
2. Salve `AWS-SCOM-MP-2.5.zip` no computador e descompacte-o.

Continue com [Implantar o AWS Management Pack \(p. 1665\)](#).

System Center 2007 R2

Antes de fazer download do AWS Management Pack, verifique se seus sistemas atendem aos seguintes requisitos e pré-requisitos do sistema.

Requisitos do sistema

- System Center Operations Manager 2007 R2
- Microsoft.Unix.Library MP versão 6.1.7000.256 ou posterior

Prerequisites

- O datacenter deve ter um computador gerenciado por agente com conectividade com a Internet que você designa como o nó observador. O nó observador deve ter a seguinte opção de proxy de agente habilitada: Allow this agent to act as a proxy and discover managed objects on other computers (Permitir que o agente aja como proxy e descubra objetos gerenciados em outros computadores). O nó observador deve ter a versão 3.5.1 do Microsoft .NET Framework ou posterior e o PowerShell 2.0 ou posterior instalados.
- A conta de ação do nó observador deve ter privilégios de administrador local no nó observador.
- Você deve garantir que o nó observador tenha o agente instalado, tenha acesso à Internet e possa se comunicar com os servidores de gerenciamento no datacenter. Para obter mais informações, consulte [Como implantar agentes do Windows](#) na documentação do Microsoft System Center.

Para fazer download do AWS Management Pack

1. No site [Suplementos da AWS para o Microsoft System Center](#), clique em SCOM 2007.
2. Salve o `AWS-MP-Setup-2.5.msi` em seu computador.

Continue com [Implantar o AWS Management Pack \(p. 1665\)](#).

Implantar o AWS Management Pack

Para poder implantar o AWS Management Pack, você deve fazer download dele. Para obter mais informações, consulte [Fazer download do AWS Management Pack \(p. 1664\)](#).

Tarefas

- [Etapa 1: Instalar o AWS Management Pack \(p. 1666\)](#)
- [Etapa 2: Configurar o nó observador \(p. 1667\)](#)
- [Etapa 3: Criar uma conta Executar como da AWS \(p. 1668\)](#)

- [Etapa 4: Executar o Assistente para Adicionar monitoramento \(p. 1672\)](#)
- [Etapa 5: Configurar portas e endpoints \(p. 1676\)](#)

Etapa 1: Instalar o AWS Management Pack

Depois de fazer download do AWS Management Pack, você deve configurá-lo para monitorar uma ou mais contas da AWS.

System Center 2012

Para instalar o AWS Management Pack

1. No console de operações, no menu Go (Acessar), clique em Administration (Administração) e, em seguida, clique em Management Packs (Pacotes de gerenciamento).
2. No painel Actions (Ações), clique em Import Management Packs (Importar pacotes de gerenciamento).
3. Na página Select Management Packs (Selecionar pacotes de gerenciamento), clique em Add (Adicionar) e, em seguida, clique em Add from disk (Adicionar do disco).
4. Na caixa de diálogo Select Management Packs to import (Selecionar pacotes de gerenciamento para importar), selecione o arquivo `Amazon.AmazonWebServices.mpb` no local onde foi feito download e, em seguida, clique em Open (Abrir).
5. Na página Select Management Packs (Selecionar pacotes de gerenciamento), sob Import list (Importar lista), selecione o pacote de gerenciamento da Amazon Web Services e clique em Install (Instalar).

Note

O System Center Operations Manager não importa nenhum pacote de gerenciamento na lista Import (Importar) que exibe um ícone Error (Erro).

6. A página Import Management Packs (Importar pacotes de gerenciamento) mostra o andamento do processo de importação. Se ocorrer um problema, selecione o pacote de gerenciamento na lista para visualizar os detalhes de status. Clique em Close.

System Center 2007 R2

Para instalar o AWS Management Pack

O pacote de gerenciamento é distribuído como um arquivo do Instalador do sistema da Microsoft, `AWS-MP-Setup.msi`. Ele contém as DLLs necessárias para o nó observador, o servidor de gerenciamento raiz e o console de Operações, bem como o arquivo `Amazon.AmazonWebServices.mp`.

1. Executar `AWS-MP-Setup.msi`.

Note

Se o servidor de gerenciamento raiz, o console de Operações e o nó observador estiverem em computadores diferentes, você deverá executar o instalador em cada computador.

2. Na tela Welcome to the Amazon Web Services Management Pack Setup Wizard (Bem-vindo ao Assistente de configuração do pacote de gerenciamento da Amazon Web Services), clique em Next (Avançar).
3. Na tela End-User License Agreement (Contrato de licença do usuário final), leia o contrato de licença e, se você aceitar os termos, marque a caixa de seleção I accept the terms in the License Agreement (Aceito os termos do contrato de licença) e clique em Next (Avançar).
4. Na tela Custom Setup (Configuração personalizada), selecione os recursos que deseja instalar e clique em Next (Avançar).

Operations Console (Console de operações)

Instala o `Amazon.AmazonWebServices.UI.Pages.dll`, registra-o no cache de assembly global (GAC) e, em seguida, instala o `Amazon.AmazonWebServices.mp`.

Root Management Server (Servidor de gerenciamento raiz)

Instala o `Amazon.AmazonWebServices.Modules.dll`, o `Amazon.AmazonWebServices.SCOM.SDK.dll` e o AWS SDK para .NET (`AWSSDK.dll`) e registra-os no GAC.

AWS Nó observador

Instala o `Amazon.AmazonWebServices.Modules.dll` e o `Amazon.AmazonWebServices.SCOM.SDK.dll` e, em seguida, instala o AWS SDK para .NET (`AWSSDK.dll`) e registra-o no GAC.

5. Na tela Ready to install Amazon Web Services Management Pack (Pronto para instalar o pacote de gerenciamento da Amazon Web Services), clique em Install (Instalar).
6. Na tela Completed the Amazon Web Services Management Pack Setup Wizard (Conclusão do Assistente de configuração do pacote de gerenciamento da Amazon Web Services), clique em Finish (Concluir).

Note

As DLLs necessárias são copiadas e registradas no GAC e o arquivo do pacote de gerenciamento (*.mp) é copiado na pasta `Program Files (x86)\Amazon Web Services Management Pack` no computador que executa o console de Operações. Em seguida, você deve importar o pacote de gerenciamento no System Center.

7. No console de operações, no menu Go (Acessar), clique em Administration (Administração) e, em seguida, clique em Management Packs (Pacotes de gerenciamento).
8. No painel Actions (Ações), clique em Import Management Packs (Importar pacotes de gerenciamento).
9. Na página Select Management Packs (Selecionar pacotes de gerenciamento), clique em Add (Adicionar) e, em seguida, clique em Add from disk (Adicionar do disco).
10. Na caixa de diálogo Select Management Packs to import (Selecionar pacotes de gerenciamento para importar), altere o diretório para `C:\Program Files (x86)\Amazon Web Services Management Pack`, selecione o arquivo `Amazon.AmazonWebServices.mp` e, em seguida, clique em Open (Abrir).
11. Na página Select Management Packs (Selecionar pacotes de gerenciamento), sob Import list (Importar lista), selecione o pacote de gerenciamento da Amazon Web Services e clique em Install (Instalar).

Note

O System Center Operations Manager não importa nenhum pacote de gerenciamento na lista Import (Importar) que exibe um ícone Error (Erro).

12. A página Import Management Packs (Importar pacotes de gerenciamento) mostra o andamento do processo de importação. Se ocorrer um problema, selecione o pacote de gerenciamento na lista para visualizar os detalhes de status. Clique em Close.

Etapa 2: Configurar o nó observador

No System Center Operations Manager 2007 R2, o nó observador executa as descobertas que vão além do computador do nó observador, portanto, você deve habilitar a opção de agente de proxy no nó observador. O agente de proxy permite que essas descobertas acessem os objetos em outros computadores.

Note

Se o sistema estiver configurado com um grande número de recursos, recomendamos que você configure um servidor de gerenciamento como o nó observador. Ter um servidor de gerenciamento de nó observador separado pode melhorar o desempenho.

Se estiver usando o System Center 2012 — Operations Manager, você poderá ignorar esta etapa.

Para habilitar o agente de proxy no System Center Operations Manager 2007 R2

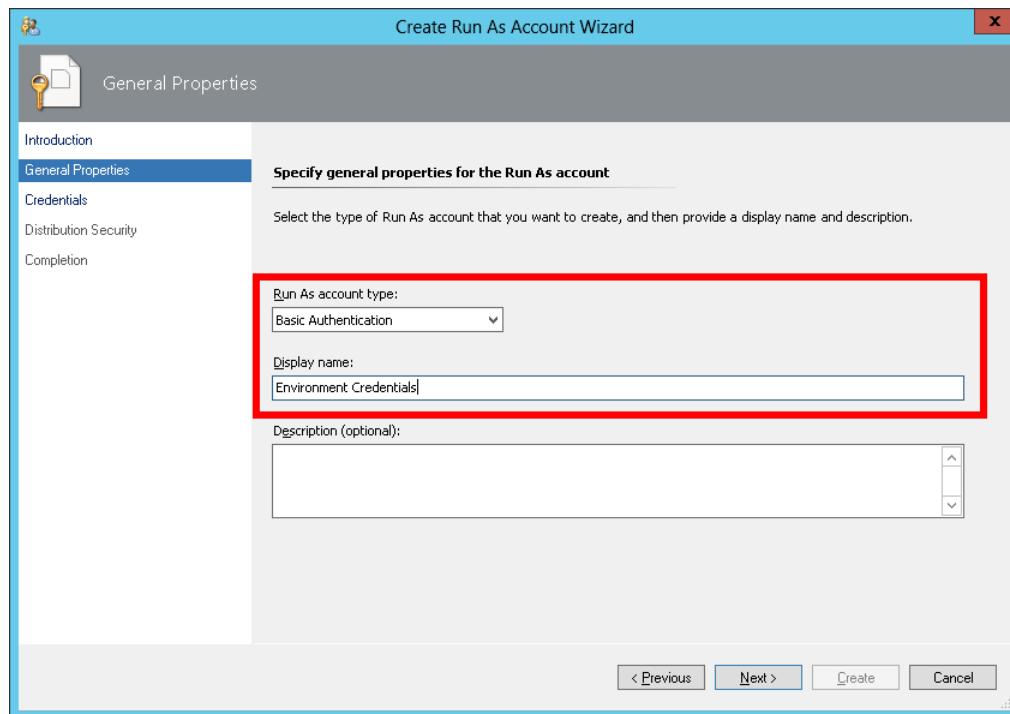
1. No console de operações, no menu Go (Acessar), clique em Administration (Administração).
2. No espaço de trabalho Administration (Administração), sob Device Management (Gerenciamento de dispositivos), clique em Agent Managed (Agente gerenciado).
3. Na lista Agent Managed (Agente gerenciado), clique com o botão direito do mouse no nó observador e clique em Properties (Propriedades).
4. Na caixa de diálogo Agent Properties (Propriedades do agente), clique na guia Security (Segurança), selecione Allow this agent to act as proxy and discover managed objects on other computers (Permitir que o agente aja como proxy e descubra objetos gerenciados em outros computadores) e clique em OK.

Etapa 3: Criar uma conta Executar como da AWS

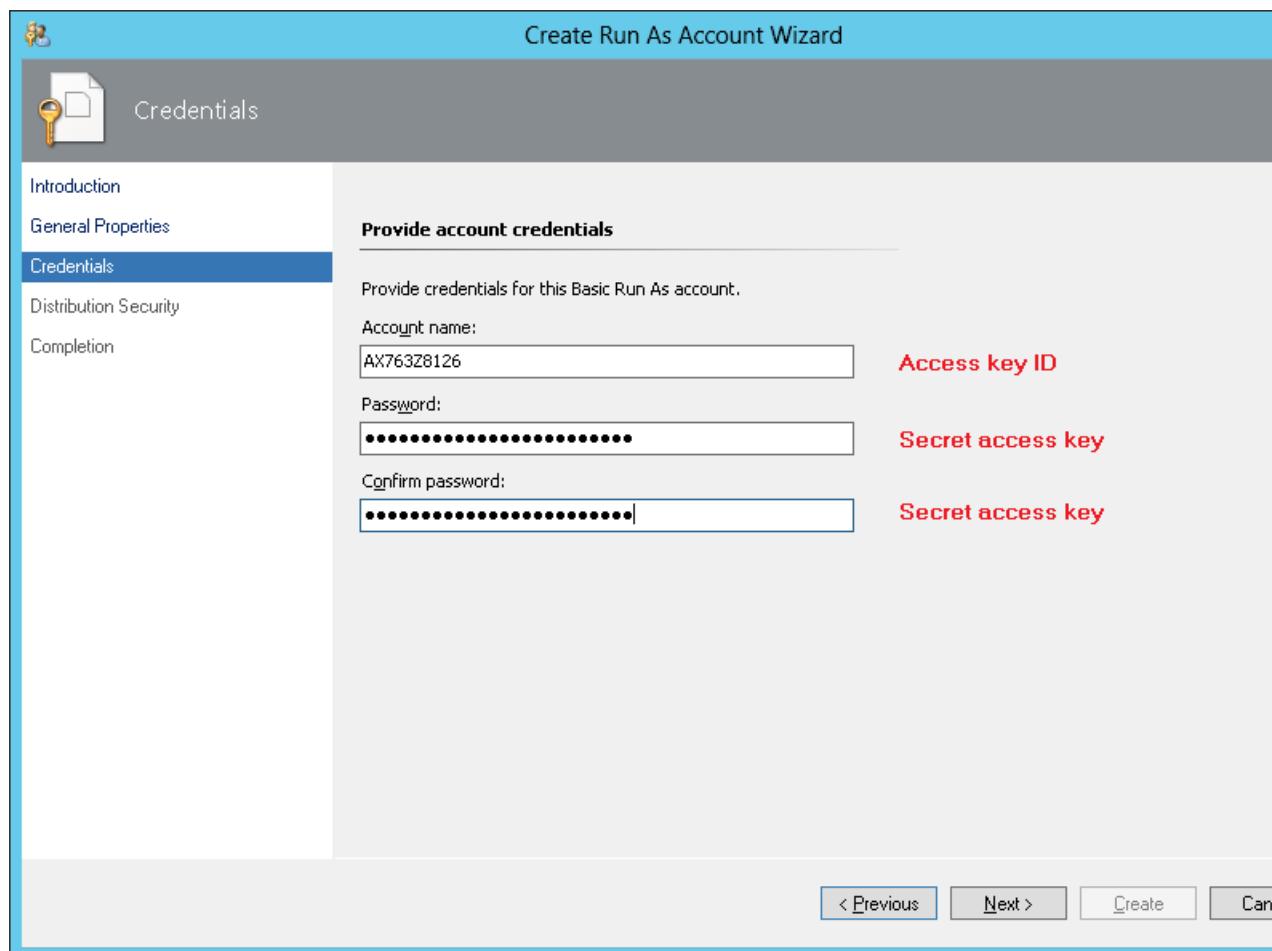
Você deve configurar as credenciais que concedem ao AWS Management Pack acesso aos recursos da AWS.

Para criar uma conta Run As do AWS

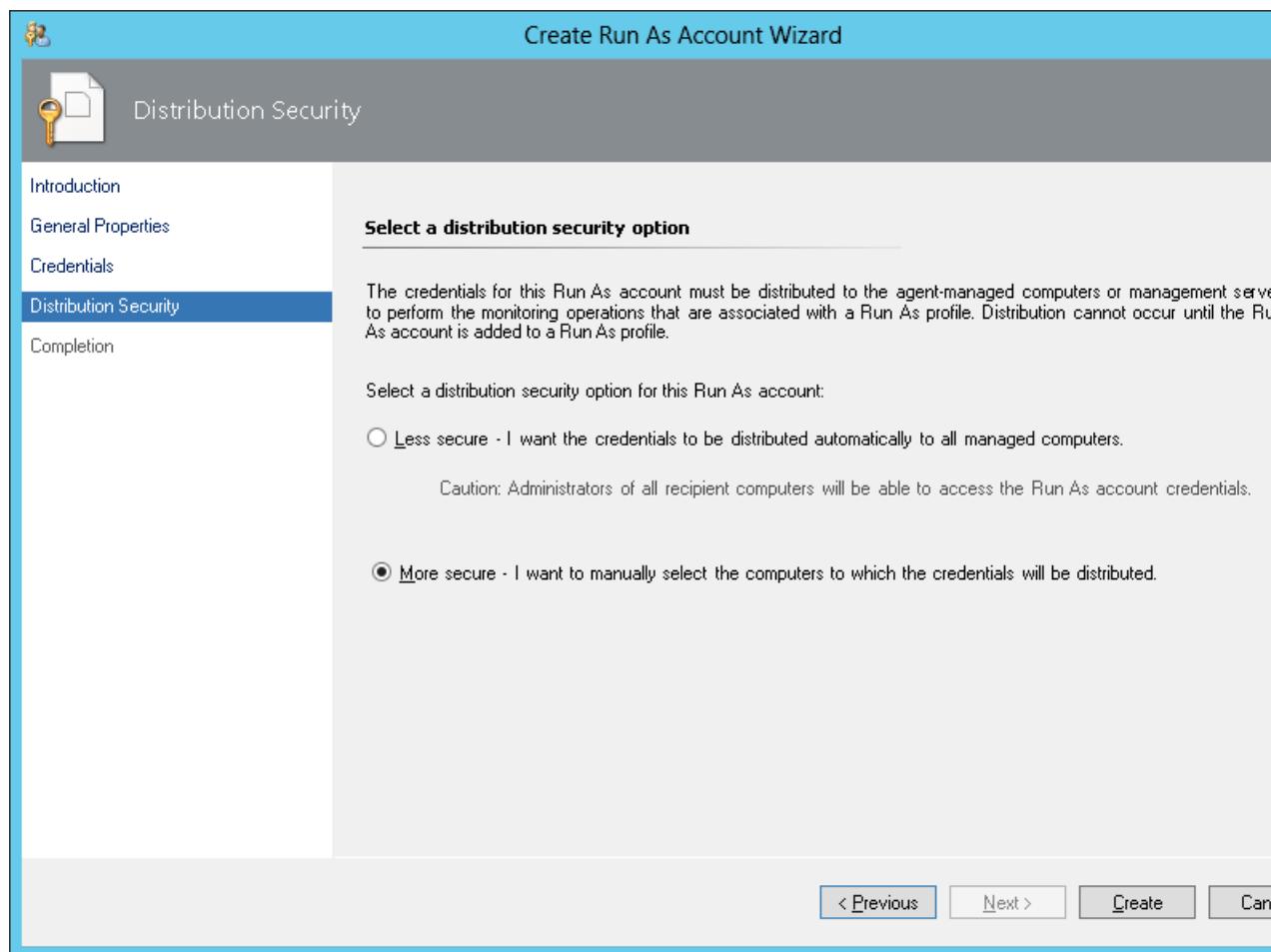
1. Recomendamos que você crie um usuário do IAM com os direitos de acesso mínimos exigidos (por exemplo, a política gerenciada da AWS ReadOnlyAccess funciona na maioria dos casos). Você precisará das chaves de acesso (ID da chave de acesso e da chave de acesso secreta) desse usuário para concluir este procedimento. Para obter mais informações, consulte [Como administrar chaves de acesso para usuários do IAM](#) no Guia do usuário do IAM.
2. No console de operações, no menu Go (Acessar), clique em Administration (Administração).
3. No espaço de trabalho Administration (Administração), expanda o nó Run As Configuration (Configuração de Executar como) e selecione Accounts (Contas).
4. Clique com o botão direito do mouse no painel Accounts (Contas) e clique em Create Run As Account (Criar conta Executar como).
5. Em Create Run As Account Wizard (Assistente de criação de conta Executar como), na página General Properties (Propriedades gerais), na lista Run As account type (Tipo da conta Executar como), selecione Basic Authentication (Autenticação básica).
6. Insira um nome de exibição (por exemplo, “Minha conta do IAM”) e uma descrição e, em seguida, clique em Next (Avançar).



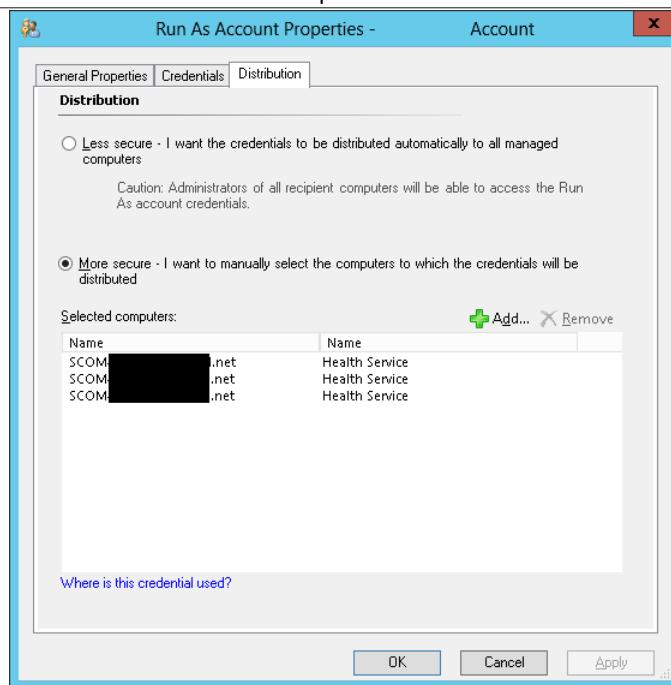
7. Na página Credentials (Credenciais), insira o ID da chave de acesso na caixa Account name (Nome da conta) e a chave de acesso secreta na caixa Password (Senha) e, em seguida, clique em Next (Avançar).



8. Na página Distribution Security (Segurança da distribuição), selecione More secure - I want to manually select the computers to which the credentials will be distributed (Mais seguro – Desejo selecionar manualmente os computadores aos quais as credenciais serão distribuídas) e clique em Create (Criar).



9. Clique em Close.
10. Na lista de contas, selecione a conta que você acabou de criar.
11. No painel Actions (Ações), clique em Properties (Propriedades).
12. Na caixa de diálogo Properties (Propriedades), verifique se a opção More Secure (Mais seguro) está selecionada e se todos os servidores de gerenciamento a serem usados para monitorar os recursos da AWS estão listados.



Etapa 4: Executar o Assistente para Adicionar monitoramento

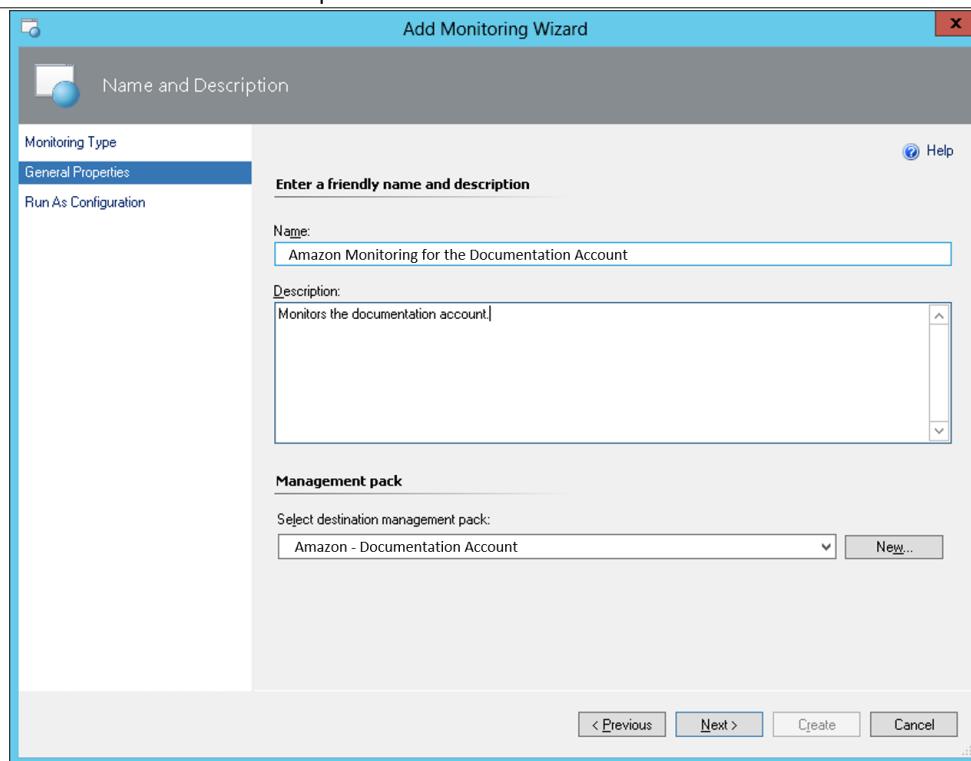
Você pode configurar o AWS Management Pack para monitorar uma conta da AWS específica usando o Assistente de adição de monitoramento, que está disponível no espaço de trabalho Authoring (Criação) do console de operações. Esse assistente cria um pacote de gerenciamento que contém as configurações para a conta da AWS a ser monitorada. Você deve executar o assistente para monitorar cada conta da AWS. Por exemplo, se quiser monitorar duas contas da AWS, você deve executar o assistente duas vezes.

System Center 2012

Para executar o Assistente para Adicionar monitoramento no System Center 2012 — Operations Manager

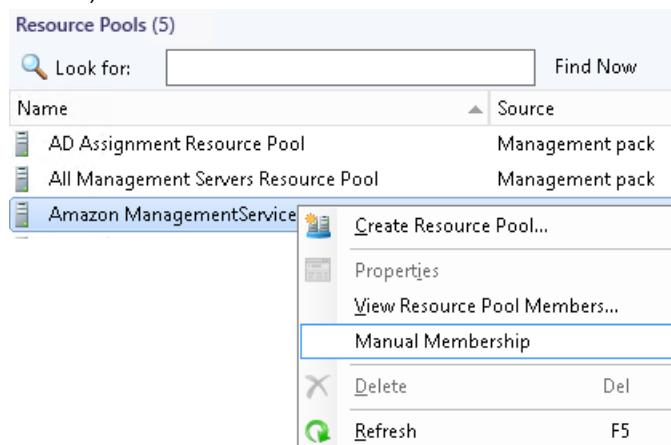
1. No console de operações, no menu Go (Acessar), clique em Authoring (Criação).
2. No espaço de trabalho Authoring (Criação), expanda o nó Management Pack Templates (Modelos de pacotes de gerenciamento), clique com o botão direito do mouse em Amazon Web Services e, em seguida, clique em Add Monitoring Wizard (Assistente de adição de monitoramento).
3. No Add Monitoring Wizard (Assistente de adição de monitoramento), na lista Select the monitoring type (Selecionar o tipo de monitoramento), selecione Amazon Web Services e clique em Next (Avançar).
4. Na página General Properties (Propriedades gerais), na caixa Name (Nome), digite um nome (por exemplo, "Meus recursos da AWS"). Na caixa Description (Descrição), digite uma descrição.
5. Na lista Select destination management pack (Selecionar pacote de gerenciamento de destino), selecione um pacote de gerenciamento existente (ou clique em New (Novo) para criar um) onde deseja salvar as configurações. Clique em Next (Próximo).

Amazon Elastic Compute Cloud Manual
 do usuário para instâncias do Windows
 Etapa 4: Executar o Assistente
 para Adicionar monitoramento

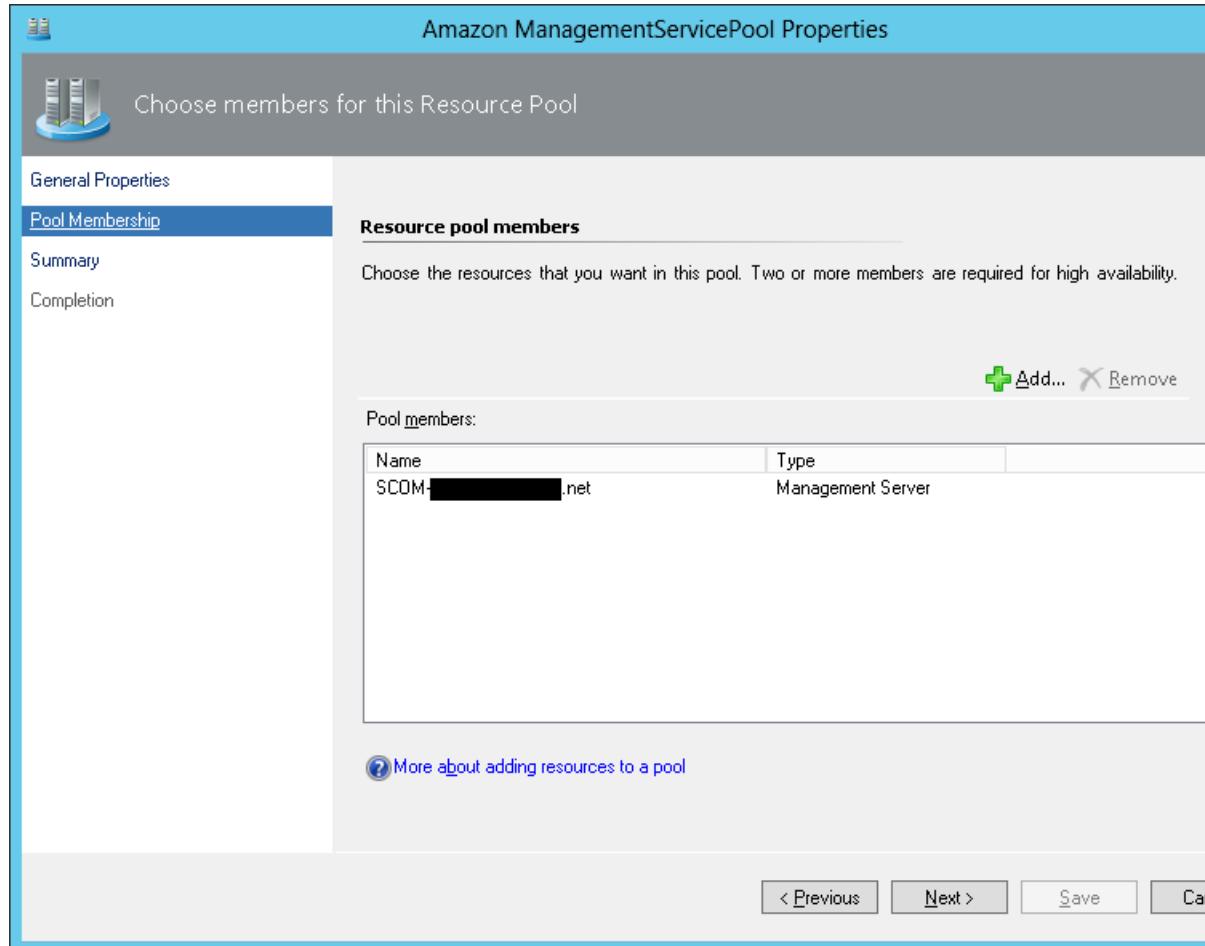


Por padrão, quando você cria um objeto de pacote de gerenciamento, desabilita uma regra ou um monitor ou cria uma substituição, o Operations Manager salva a configuração no pacote de gerenciamento padrão. Como uma melhor prática, você deve criar um pacote de gerenciamento separado para cada pacote de gerenciamento selado que deseja personalizar, em vez de salvar as configurações personalizadas no pacote de gerenciamento padrão.

6. O AWS Management Pack cria automaticamente um grupo de recursos e adiciona os servidores de gerenciamento a ele. Para controlar a associação ao servidor, faça as seguintes alterações:
 - a. Clique em Administration (Administração) no menu Go (Acessar).
 - b. Clique no nó Resource Pools (Grupos de recursos).
 - c. Clique com o botão direito do mouse em AWSResource Pool (Grupo de recursos da AWS), no painel Resource Pools (Grupos de recursos), e selecione Manual Membership (Associação manual).



-
- d. Clique com o botão direito do mouse em AWS Resource Pool (Grupo de recursos da AWS), no painel Resource Pools (Grupos de recursos), e selecione Properties (Propriedades).
 - e. Na página Pool Membership (Associação ao grupo), remova os servidores de gerenciamento que não devem monitorar recursos da AWS.



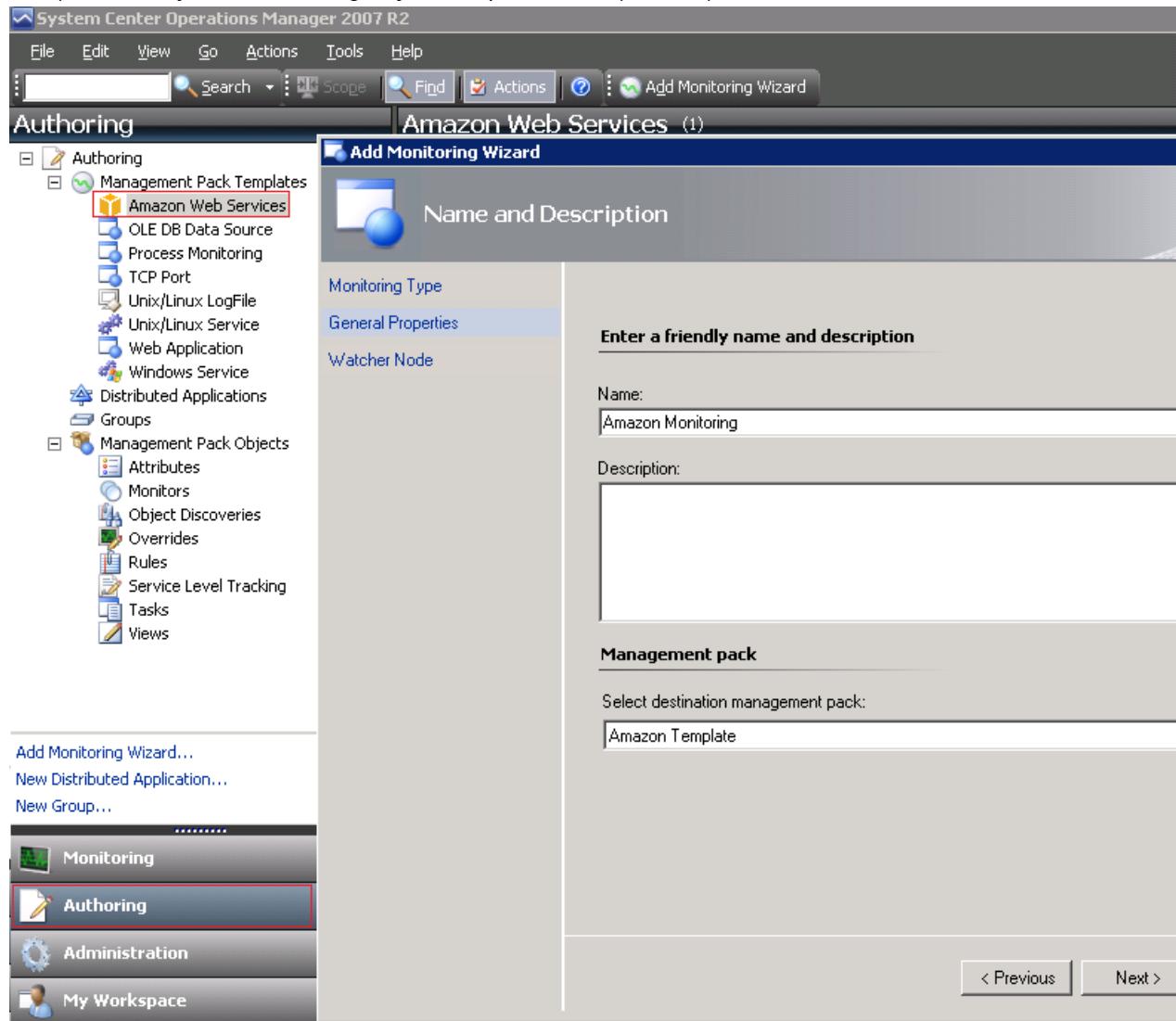
- 7. Após a configuração do AWS Management Pack, será exibida uma subpasta da pasta **Amazon Web Services** no espaço de trabalho Monitoring (Monitoramento) do console de operações.

System Center 2007 R2

Para executar o Assistente para Adicionar monitoramento no System Center Operations Manager 2007

1. No console de operações, no menu Go (Acessar), clique em Authoring (Criação).
2. No espaço de trabalho Authoring (Criação), expanda o nó Management Pack Templates (Modelos de pacotes de gerenciamento), clique com o botão direito do mouse em Amazon Web Services e, em seguida, clique em Add Monitoring Wizard (Assistente de adição de monitoramento).
3. No Add Monitoring Wizard (Assistente de adição de monitoramento), na lista Select the monitoring type (Selecionar o tipo de monitoramento), selecione Amazon Web Services e clique em Next (Avançar).
4. Na página General Properties (Propriedades gerais), na caixa Name (Nome), digite um nome (por exemplo, "Meus recursos da AWS"). Na caixa Description (Descrição), digite uma descrição.

-
5. Na lista suspensa Select destination management pack (Selecionar pacote de gerenciamento de destino), selecione um pacote de gerenciamento existente (ou clique em New (Novo) para criar um novo) onde deseja salvar as configurações. Clique em Next (Próximo).



Por padrão, quando você cria um objeto de pacote de gerenciamento, desabilita uma regra ou um monitor ou cria uma substituição, o Operations Manager salva a configuração no pacote de gerenciamento padrão. Como uma melhor prática, você deve criar um pacote de gerenciamento separado para cada pacote de gerenciamento selado que deseja personalizar, em vez de salvar as configurações personalizadas no pacote de gerenciamento padrão.

6. Na página Watcher Node Configuration (Configuração do nó observador), na lista Watcher Node (Nó observador), selecione um computador gerenciado por agente para atuar como o nó observador.
7. Na lista suspensa Select AWS Run As account (Selecionar conta Executar como da AWS), selecione a conta Executar como criada anteriormente e clique em Create (Criar).
8. Depois de ser configurado, o AWS Management Pack primeiro descobre o nó observador. Para verificar se o nó observador foi descoberto com êxito, navegue até o espaço de trabalho Monitoring (Monitoramento) no console de operações. Você deve ver uma nova pasta Amazon Web Services e uma subpasta Amazon Watcher Nodes sob ela. Essa subpasta exibe os nós observadores. O AWS Management Pack verifica e monitora automaticamente a conectividade do nó observador com

a AWS. Quando o nó observador é descoberto, ele é mostrado nesta lista. Quando o nó observador está pronto, seu estado muda para **Healthy**.

Note

Para estabelecer uma conectividade com a AWS, o AWS Management Pack requer que você implante o AWS SDK para .NET, os módulos e os scripts no nó observador. Isso pode demorar cerca de dez minutos. Se o nó observador não aparecer ou se você vir o estado como **Not Monitored**, verifique a conectividade com a Internet e as permissões do IAM. Para obter mais informações, consulte [Solucionar problemas do AWS Management Pack \(p. 1698\)](#).

9. Após o nó observador ser descoberto, as descobertas dependentes são acionadas e os recursos da AWS são adicionados ao espaço de trabalho Monitoring (Monitoramento) do console de operações.

A descoberta de recursos da AWS deve ser concluída em vinte minutos. Esse processo pode demorar mais tempo, dependendo do ambiente do Operations Manager, do ambiente da AWS, da carga no servidor de gerenciamento e da carga no nó observador. Para obter mais informações, consulte [Solucionar problemas do AWS Management Pack \(p. 1698\)](#).

Etapa 5: Configurar portas e endpoints

O AWS Management Pack para Microsoft System Center deve se comunicar com os serviços da AWS para monitorar a performance desses serviços e para fornecer alertas no System Center. Para que o monitoramento tenha êxito, você deve configurar o firewall nos servidores do Management Pack para permitir chamadas HTTP de saída nas portas 80 e 443 aos endpoints da AWS para os serviços a seguir.

Isso permite o monitoramento para os seguintes serviços da AWS:

- Amazon Elastic Compute Cloud (EC2)
- Elastic Load Balancing
- Amazon EC2 Auto Scaling
- AWS Elastic Beanstalk
- Amazon CloudWatch
- AWS CloudFormation

O AWS Management Pack usa as APIs públicas no AWS SDK para .NET para recuperar informações desses serviços nas portas 80 e 443. Faça login em cada servidor e habilite as regras de saída do firewall para as portas 80 e 443.

Se o aplicativo do firewall oferecer suporte a configurações mais detalhadas, você poderá configurar endpoints específicos para cada serviço. Um endpoint é uma URL que é o ponto de entrada para um serviço da Web. Por exemplo, o ec2.us-west-2.amazonaws.com é um ponto de entrada para o serviço do Amazon EC2. Para configurar endpoints no firewall, [localize as URLs específicas ao endpoint](#) para os serviços da AWS que você estiver executando e especifique os endpoints na aplicação de firewall.

Usar o AWS Management Pack

Você pode usar o AWS Management Pack para monitorar a integridade dos recursos da AWS.

Tópicos

- [Views \(p. 1677\)](#)

- [Discoveries \(p. 1691\)](#)
- [Monitors \(p. 1692\)](#)
- [Rules \(p. 1693\)](#)
- [Events \(p. 1693\)](#)
- [Modelo de integridade \(p. 1694\)](#)
- [Personalizar o AWS Management Pack \(p. 1696\)](#)

Views

O AWS Management Pack fornece as seguintes visualizações, que são exibidas no espaço de trabalho de Monitoring (Monitoramento) do console de operações.

Visualizações

- [Instâncias do EC2 \(p. 1677\)](#)
- [Volumes do Amazon EBS \(p. 1679\)](#)
- [Elastic Load Balancers \(p. 1681\)](#)
- [AWS Elastic BeanstalkAplicativos do \(p. 1683\)](#)
- [AWS CloudFormation Pilhas do \(p. 1685\)](#)
- [Visualizações de desempenho da Amazon \(p. 1687\)](#)
- [Alarms de métricas do Amazon CloudWatch \(p. 1688\)](#)
- [AWSAlertas da \(p. 1689\)](#)
- [Nós observadores \(System Center Operations Manager 2007 R2\) \(p. 1690\)](#)

Instâncias do EC2

Visualize o estado de integridade das instâncias do EC2 de uma conta específica da AWS, em todas as zonas de disponibilidade e regiões. A visualização também inclui instâncias do EC2 que executam em uma nuvem privada virtual (VPC). O AWS Management Pack recupera tags, portanto, você pode pesquisar e filtrar a lista usando essas tags.

The screenshot shows the SCOM 2012 Operations Manager interface with the title bar "EC2 Instances - scom-2012 - Operations Manager". The left pane is titled "Monitoring" and contains a tree view of monitoring categories: Monitoring, Active Alerts, Discovered Inventory, Distributed Applications, Task Status, UNIX/Linux Computers, Windows Computers, Agentless Exception Monitoring, amazon, Amazon Web Services, Personal AWS Account, All Performance, AWS Alerts, CloudFormation Stacks, CloudWatch Metric Alarms, EBS Volumes, EBS Volumes Performance, EC2 Instances, EC2 Instances Performance, Elastic Beanstalk Applications, Elastic Load Balancers, Elastic Load Balancers Performance, and Other Metrics. Below the tree view are buttons for "Show or Hide Views...", "New View >", and a list of recent views: Monitoring, Authoring, Administration, and My Workspace. The right pane is titled "EC2 Instances (103)" and displays a table of 103 instances. The columns are State, Maintenance, and Name. The table includes rows for various instance types and names, such as "Win 2012 R2 m3", "ARP - Test", "Classic", "SCOM 2007 All", "Default-Environment", "SCOM 2012 Environment - DC", "piops", "SCVMM - All in one", "applicationTwo-env", "SCOM 2012 Environment - MS 1", "SCOM 2007 DC", "SCOM 2012 Environment - SQL", and "metricgathertest". A "Detail View" section is shown for the selected instance "Default-Environment", displaying its properties: Display Name (Default-Environment), Full Path Name (Default-Environment), Region (us-west-2), Configuration ID, Instance ID, Availability Zone (us-west-2c), Image ID, Private DNS Name, Public DNS Name, Instance Type (t1.micro), Private IP Address, Public IP Address, Security Group IDs, and Security Groups.

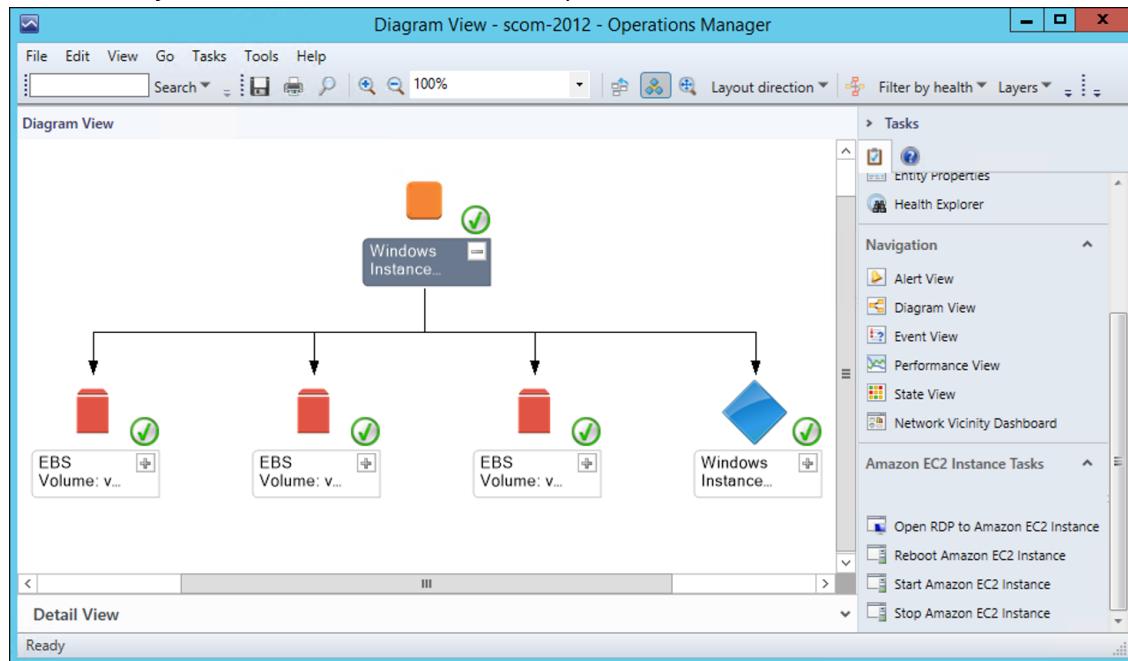
EC2 Instances (103)		
State	Maintain...	Name
Healthy		Win 2012 R2 m3
Healthy		ARP - Test
Healthy		Classic
Healthy		SCOM 2007 All
Healthy		Default-Environment
Critical		SCOM 2012 Environment - DC
Healthy		piops
Healthy		SCVMM - All in one
Healthy		applicationTwo-env
Healthy		SCOM 2012 Environment - MS 1
Healthy		SCOM 2007 DC
Healthy		SCOM 2012 Environment - SQL
Healthy		metricgathertest

Quando você seleciona uma instância do EC2, você pode executar tarefas de integridade da instância:

- Open Amazon Console (Abrir console da Amazon): inicia o AWS Management Console em um navegador da web.
- Open RDP to Instance (Abrir RDP para instância do Amazon EC2): abre uma conexão RDP para a instância Windows selecionada.
- Reboot Instance (Reiniciar instância do Amazon EC2): reinicia a instância do EC2 selecionada.
- Start Instance (Iniciar instância do Amazon EC2): inicia a instância do EC2 selecionada.
- Stop Instance (Interromper instância do Amazon EC2): interrompe a instância do EC2 selecionada.

Visualização de diagrama de instâncias do EC2

Mostra a relação de uma instância com outros componentes.



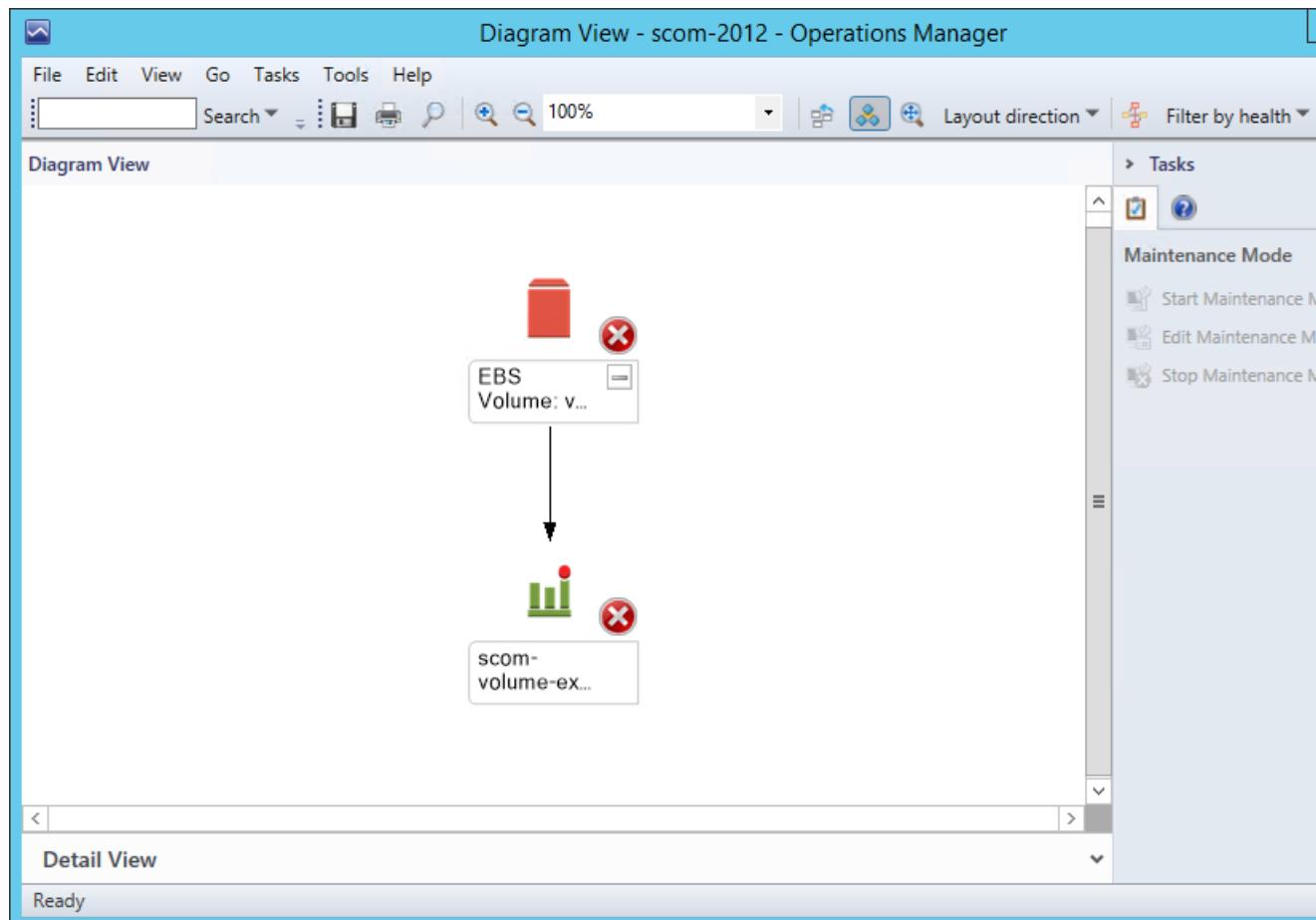
Volumes do Amazon EBS

Mostra o estado de integridade dos volumes do Amazon EBS de uma conta específica da AWS em todas as zonas de disponibilidade e regiões.

The screenshot shows the Microsoft System Center Operations Manager (SCOM) interface. The title bar reads "EBS Volumes - scom-2012 - Operations Manager". The left pane is a navigation tree under "Monitoring" with several collapsed categories like "Active Alerts", "Discovered Inventory", etc., and expanded categories like "Agentless Exception Monitoring" and "Amazon Web Services". Under "Amazon Web Services", the "EBS Volumes" node is selected. The right pane displays a table titled "EBS Volumes (214)". The table has columns: State, Maintenance, Display Name, Volume ID, and Availability. A search bar at the top of the table says "Look for: EBS Volume: vo...". One row in the table is highlighted with a red error icon and the status "Critical". The "Display Name" column lists various EBS volumes, and the "Volume ID" column shows their respective IDs. Below the table, a "Detail View" section is open for one of the EBS volumes, showing properties like "Display Name", "Full Path Name", "Region", "Volume ID", "Account Guid", "Availability Zone", "Size", "IOPS", "Attachments", "Snapshot ID", "Volume Type", "Create Time", and "Tags". The "Volume Type" is listed as "gp2". The "Create Time" is "1/19/2015 6:35:58 PM". The "Tags" section is currently empty.

Visualização de diagrama de volumes do Amazon EBS

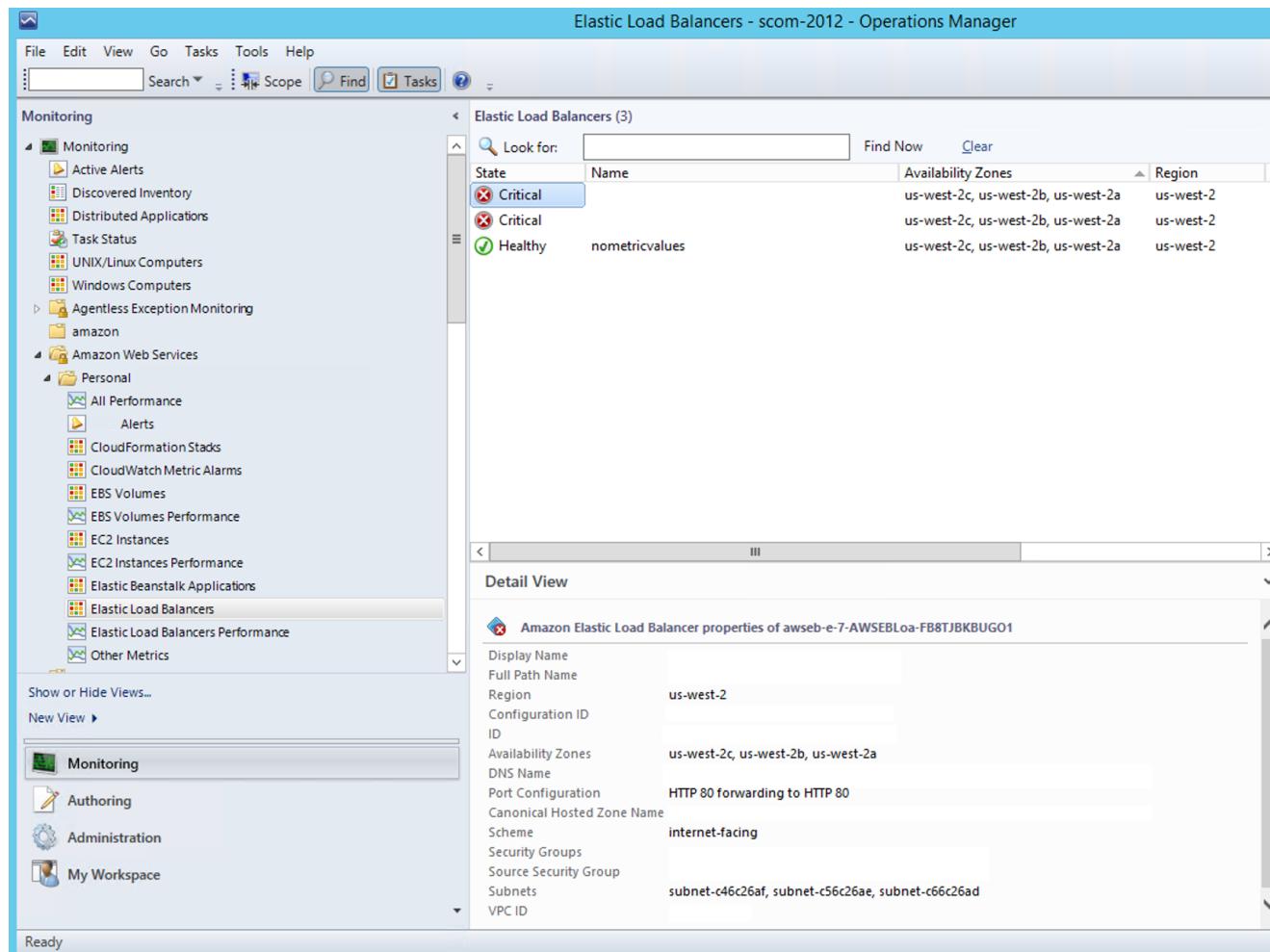
Mostra um volume do Amazon EBS e todos os alarmes associados. A ilustração a seguir mostra um exemplo:



Elastic Load Balancers

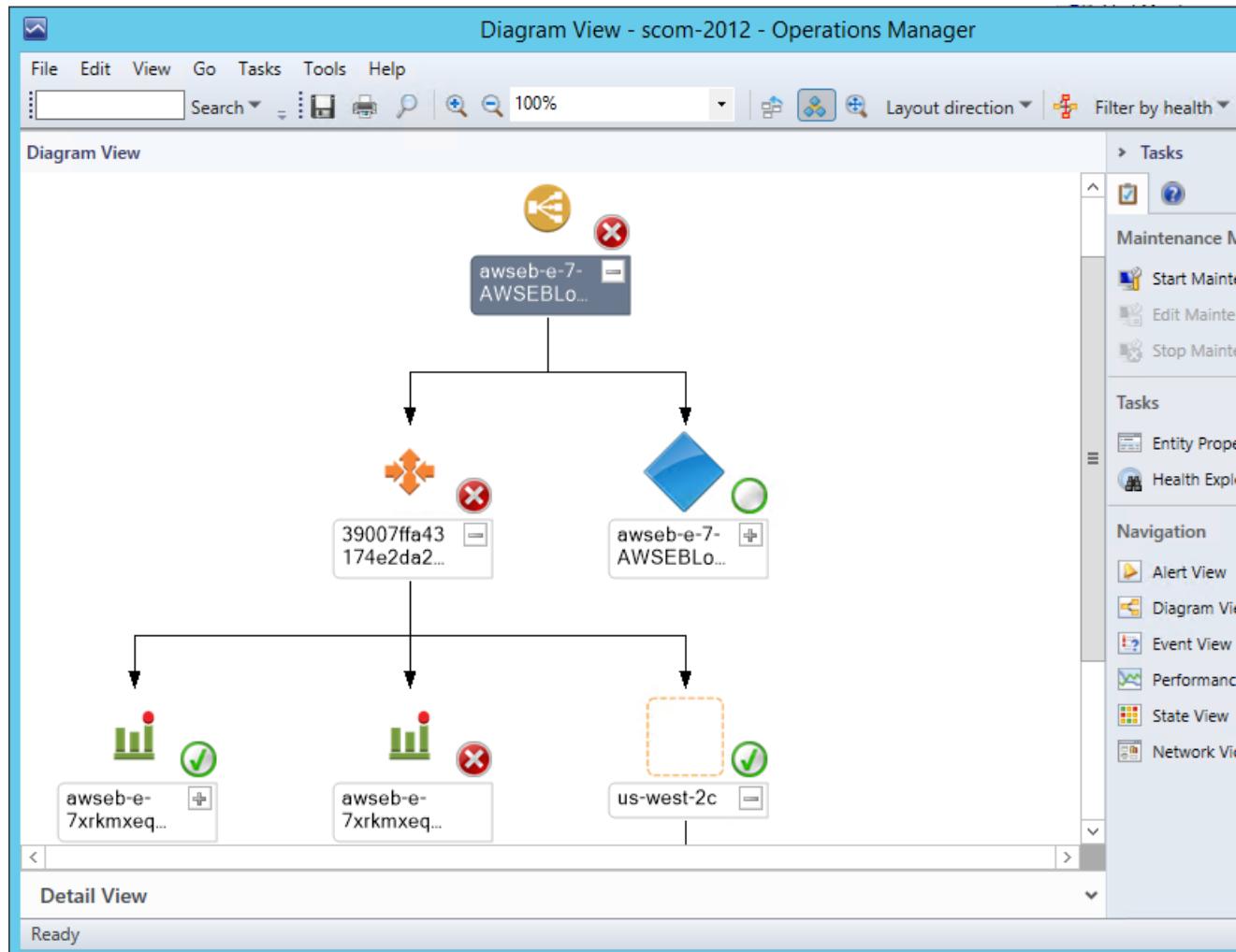
O estado de integridade de todos os balanceadores de carga de uma conta específica da AWS em todas as regiões.

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Views



Visualização de diagrama do Elastic Load Balancing

Mostra a relação do Elastic Load Balancing com outros componentes. A ilustração a seguir mostra um exemplo:



AWS Elastic Beanstalk Aplicativos do

Mostra o estado de todos os aplicativos do AWS Elastic Beanstalk descobertos.

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Views

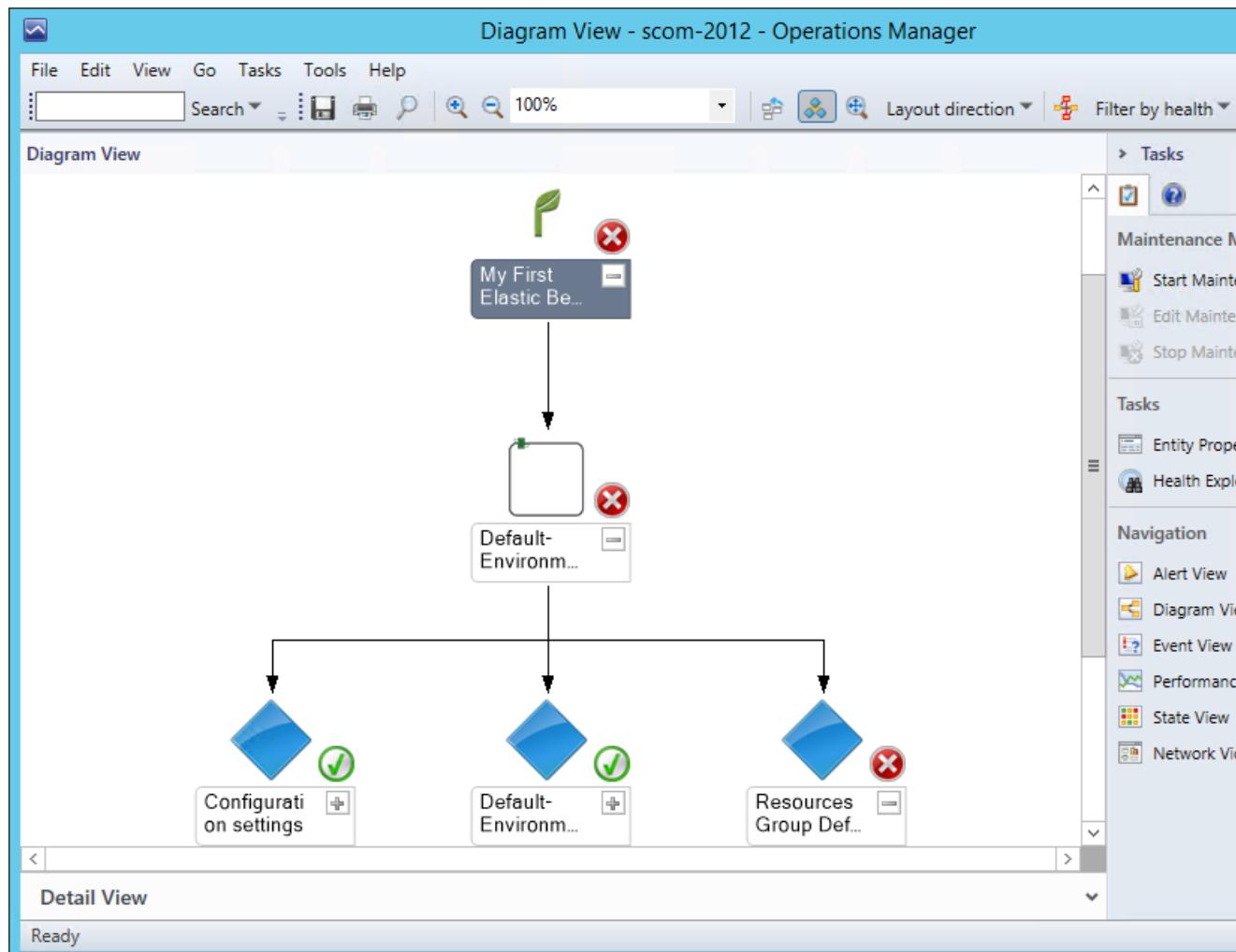
The screenshot shows the 'Elastic Beanstalk Applications - scom-2012 - Operations Manager' window. The left sidebar has a 'Monitoring' section with various sub-options like Active Alerts, Discovered Inventory, Distributed Applications, Task Status, etc. Below that are sections for Agentless Exception Monitoring, Amazon Web Services, and Personal metrics. The main area displays a table titled 'Elastic Beanstalk Applications (2)' with two entries:

State	Application Name	Application Environment	Date Created	Date Updated
Critical	application two	Critical	2/19/2015 4:52:...	2/19/2015 4:52:...
Critical	My First Elastic Beanstalk Application	Critical	4/9/2014 7:52:1...	4/9/2014 7:52:1...

On the right side, there are 'Tasks' and 'Navigation' panels. The 'Tasks' panel includes options like 'Start Maintenance Mode...', 'Stop Maintenance Mode...', and 'Personalize view...'. The 'Navigation' panel lists Alert View, Diagram View, Event View, Performance View, State View, and Network Vicinity Dashboard.

AWS Elastic Beanstalk Visualização do diagrama de aplicativos do

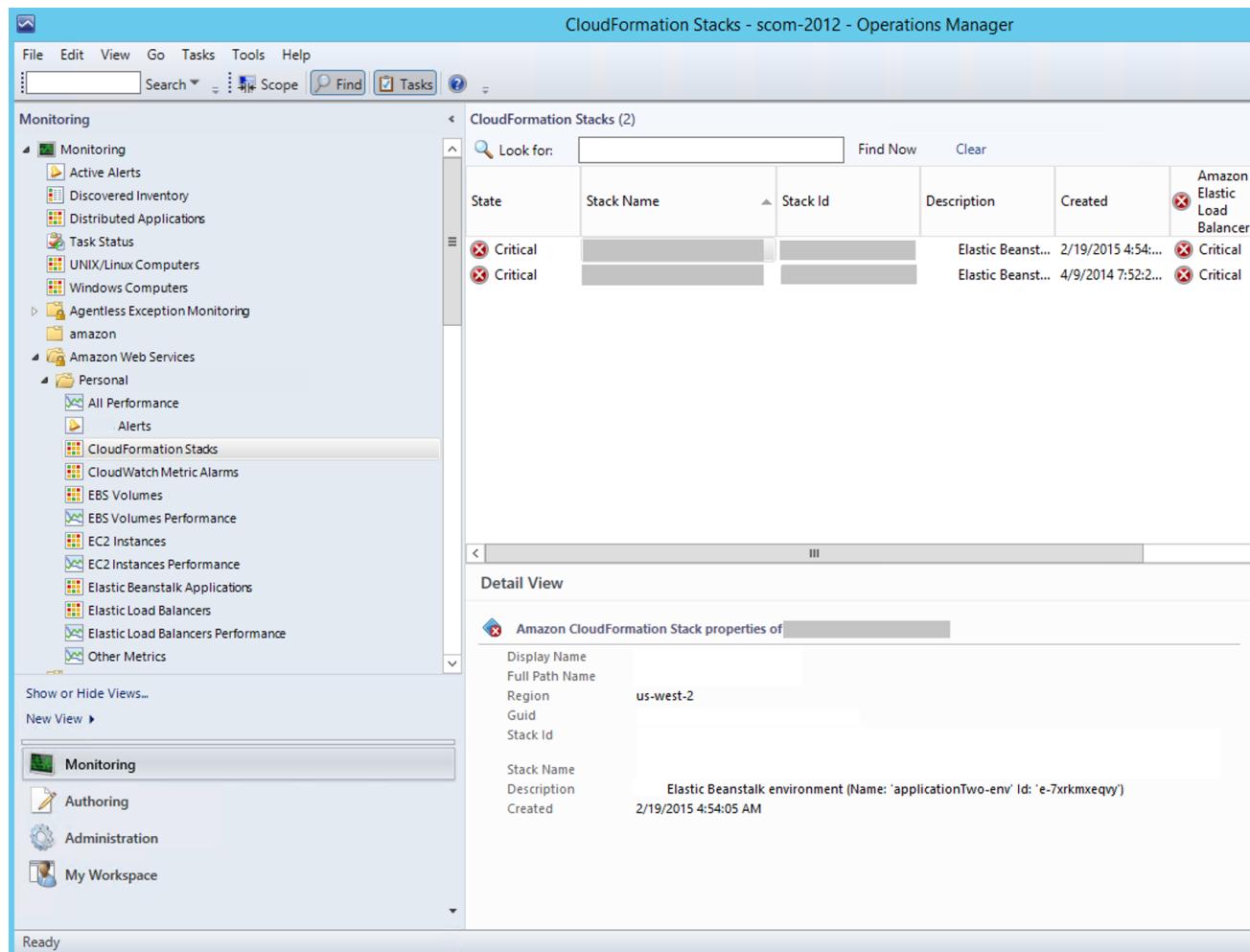
Mostra o aplicativo do AWS Elastic Beanstalk, o ambiente do aplicativo, a configuração do aplicativo e os objetos dos recursos do aplicativo.



AWS CloudFormation Pilhas do

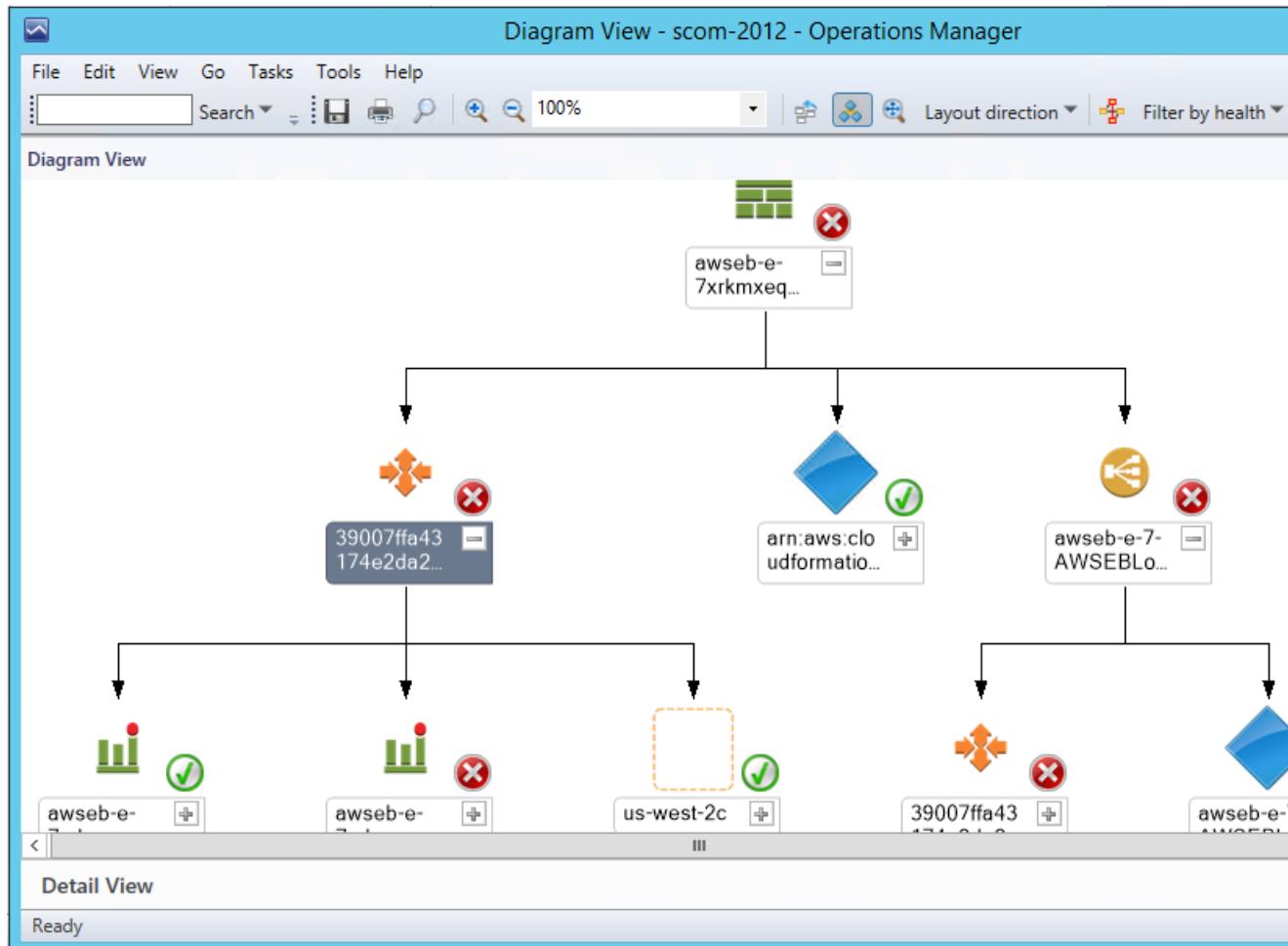
Mostra o estado de integridade de todas as pilhas do AWS CloudFormation para uma conta específica da AWS em todas as regiões.

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Views



AWS CloudFormation Visualização do diagrama de pilhas do

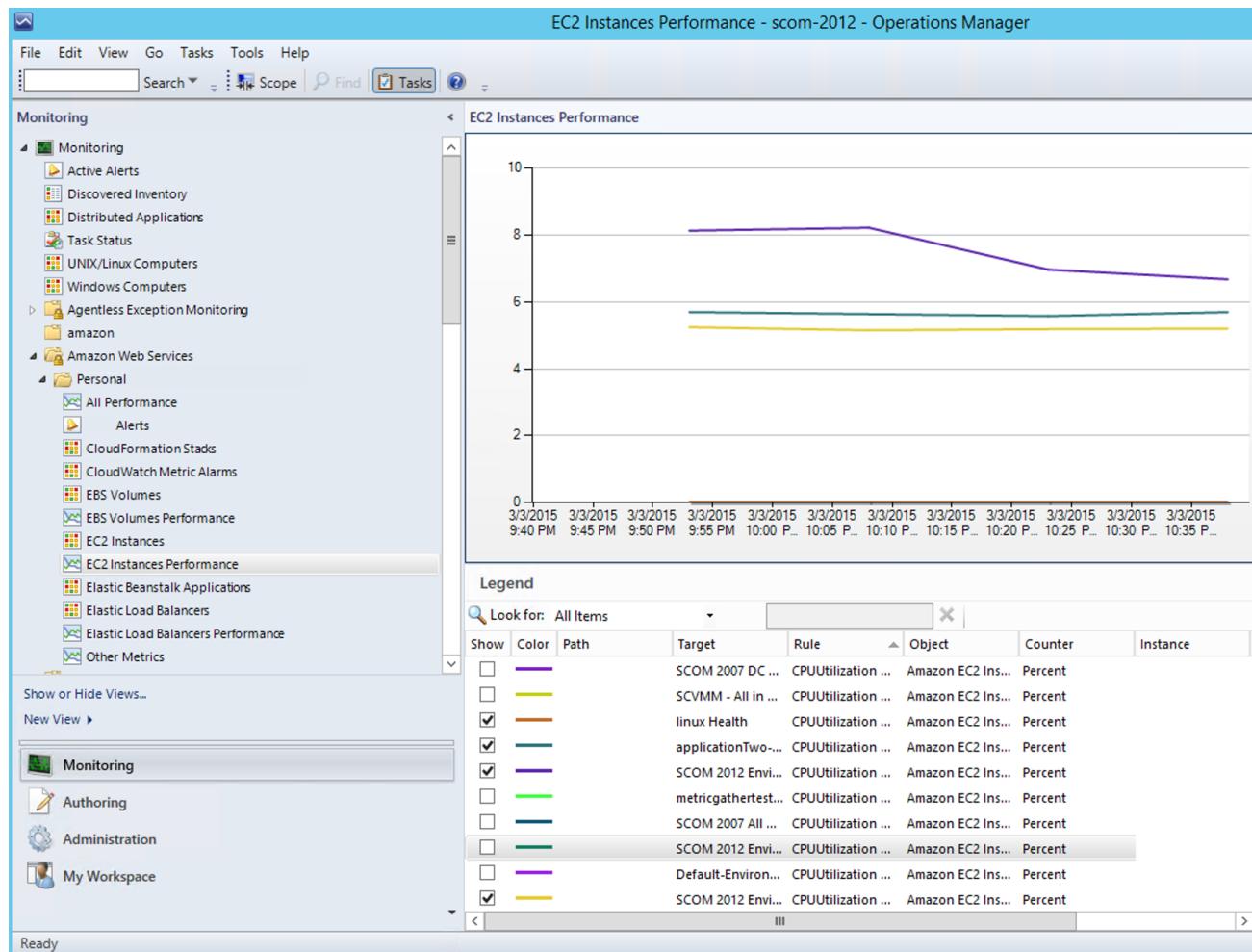
Mostra a relação das pilhas do AWS CloudFormation com outros componentes. Uma pilha do AWS CloudFormation pode conter recursos do Amazon EC2 ou do Elastic Load Balancing. A ilustração a seguir mostra um exemplo:



Visualizações de desempenho da Amazon

Mostra métricas do Amazon CloudWatch para o Amazon EC2, o Amazon EBS e o Elastic Load Balancing, métricas personalizadas e métricas criadas de alarmes do CloudWatch. Além disso, há visualizações de desempenho separadas para cada recurso. A visualização de desempenho Other Metrics (Outras métricas) contém métricas personalizadas e métricas criadas de alarmes do CloudWatch. Para obter mais informações sobre essas métricas, consulte [AWS Services That Publish CloudWatch Metrics](#) (Serviços da AWS que publicam métricas do CloudWatch), no Guia do usuário do Amazon CloudWatch. A ilustração a seguir mostra um exemplo.

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Views



Alarmes de métricas do Amazon CloudWatch

Mostra os alarmes do Amazon CloudWatch relacionados aos recursos da AWS descobertos.

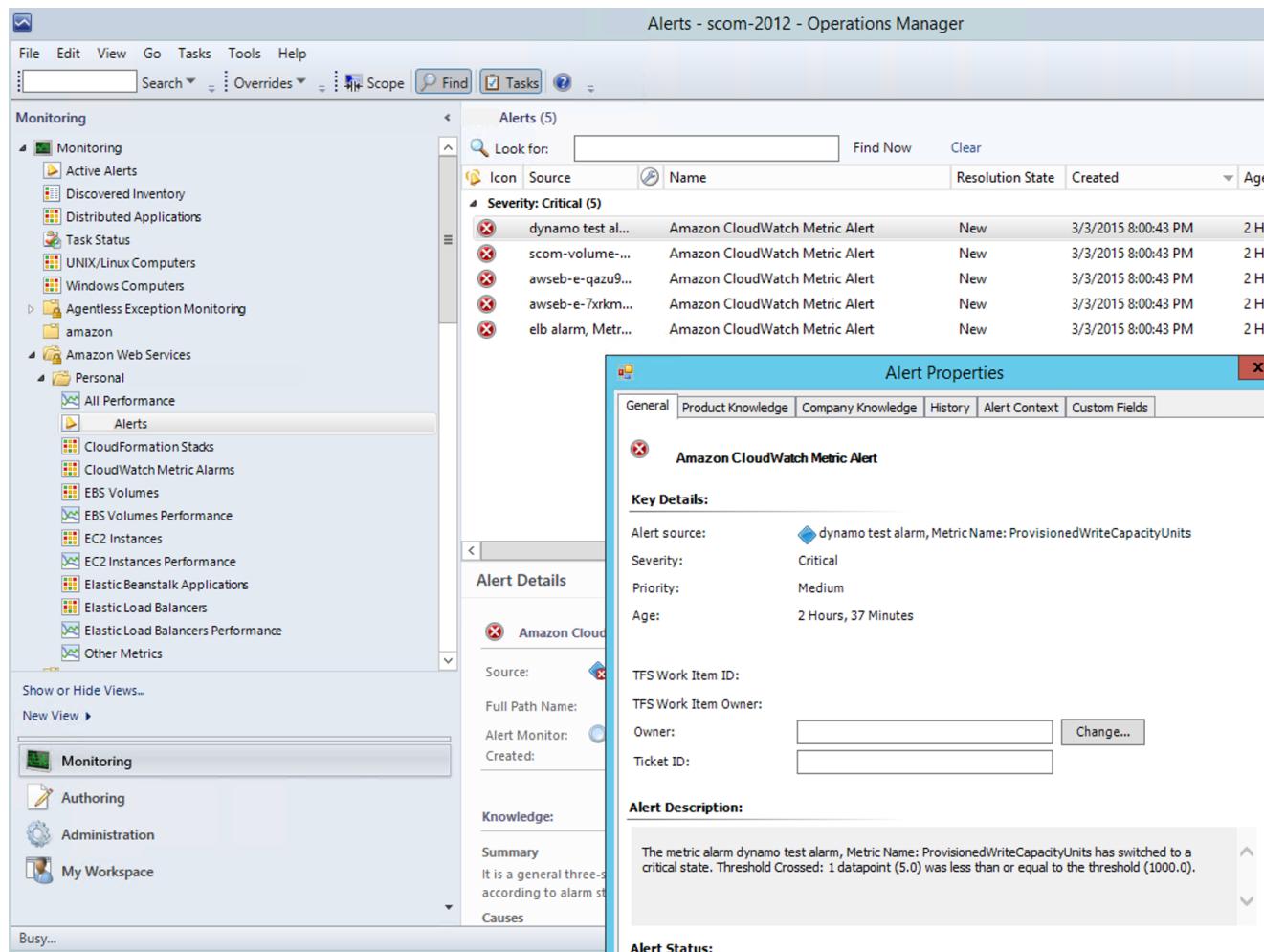
The screenshot shows the 'CloudWatch Metric Alarms' view in the Operations Manager. The left sidebar has a tree view under 'Monitoring' with categories like Active Alerts, Discovered Inventory, Distributed Applications, Task Status, UNIX/Linux Computers, Windows Computers, Agentless Exception Monitoring, amazon, Amazon Web Services, Personal, and CloudWatch Metric Alarms. The 'CloudWatch Metric Alarms' node is selected. The main pane displays a table titled 'CloudWatch Metric Alarms (11)' with columns: State, Alarm Name, Metric Name, Condition, and Description. The table lists 11 alarms, mostly critical, including 'dynamo test alarm', 'scom-volume-exists-test', and various AWS services like 'awseb-e-qazu95f2zm-stack-A...'. Below the table is a 'Detail View' for the 'dynamo test alarm', showing its properties: Display Name (dynamo test alarm, Metric Name: ProvisionedWriteCapacityUnits), Full Path Name (dynamo test alarm, Metric Name: ProvisionedWriteCapacityUnits), Region (us-west-2), Alarm ID (arn:aws:cloudwatch:us-west-2:946130359068:alarm:dynamo test alarm 39007ffa43174e2da200cb945151a2bd), Description (should always alarm), Condition (ProvisionedWriteCapacityUnits <= 1000), Alarm Name (dynamo test alarm), Metric Name (ProvisionedWriteCapacityUnits), Namespace (AWS/DynamoDB), Threshold (1000), and Unit.

State	Alarm Name	Metric Name	Condition	Description
✖ Critical	dynamo test alarm	ProvisionedWriteCapacityUn...	ProvisionedWriteCapacityUnits <= 10...	should always alarm
✖ Critical	scom-volume-exists-test	VolumeReadBytes	VolumeReadBytes >= 0	
✖ Critical	awseb-e-qazu95f2zm-stack-A...	NetworkOut	NetworkOut < 2000000	AWS/...
✖ Critical	elb alarm	HealthyHostCount	HealthyHostCount <= 10	should always alarm
✖ Critical	awseb-e-7xrkmxeqvy-stack-A...	NetworkOut	NetworkOut < 2000000	AWS/...
✓ Healthy	awseb-e-qazu95f2zm-stack-A...	NetworkOut	NetworkOut > 6000000	AWS/...
✓ Healthy	awseb-e-7xrkmxeqvy-stack-A...	NetworkOut	NetworkOut > 6000000	AWS/...
✓ Healthy	testalarm	VolumeReadBytes	VolumeReadBytes <= 50000	AWS/...
✓ Healthy	az_alarm	Latency	Latency <= 1	AWS/...
✓ Healthy	awsec2-i-cc4811c4-High-CPU...	CPUUtilization	CPUUtilization < 80	AWS/...
✓ Healthy	scom-bug-alarm	CPUUtilization	CPUUtilization <= 80	AWS/...

AWSAlerts da

Mostra os alertas que o pacote de gerenciamento da AWS produz quando a integridade de um objeto estiver em um estado crítico.

Amazon Elastic Compute Cloud Manual
do usuário para instâncias do Windows
Views



Nós observadores (System Center Operations Manager 2007 R2)

Visualize o estado de integridade dos nós observadores em todas as contas da AWS que estiverem sendo monitoradas. O estado Healthy (Integro) significa que o nó observador está configurado e pode se comunicar com a AWS.



Discoveries

As descobertas são os recursos da AWS que são monitorados pelo AWS Management Pack. O AWS Management Pack descobre os seguintes objetos:

- Instâncias do Amazon EC2
- Volumes do EC2
- Load balancers ELB
- AWS CloudFormation Pilhas do
- Alarmes do Amazon CloudWatch
- AWS Elastic BeanstalkAplicativos do
- Grupos e zonas de disponibilidade do Amazon EC2 Auto Scaling

As métricas do Amazon CloudWatch são geradas pelos seguintes recursos:

- Instância do Amazon EC2
- Volume do EBS
- Elastic Load Balancing
- Métricas personalizadas do Amazon CloudWatch
- Métricas de alarmes existentes do Amazon CloudWatch

Para a descoberta de métricas do Amazon CloudWatch, as seguintes diretrizes se aplicam:

- AWS CloudFormation As pilhas do não têm nenhuma métrica padrão do Amazon CloudWatch.
- As instâncias interrompidas do Amazon EC2 ou os volumes não utilizados do Amazon EBS não geram dados para suas métricas padrão do Amazon CloudWatch.
- Depois de iniciar uma instância do Amazon EC2, pode demorar até 30 minutos para que as métricas do Amazon CloudWatch apareçam no Operations Manager.

- O Amazon CloudWatch retém os dados de monitoramento por duas semanas, mesmo que os recursos da AWS tenham sido encerrados. Esses dados aparecem no Operations Manager.
- Um alarme existente do Amazon CloudWatch para um recurso não compatível criará uma métrica e a associará ao alarme do Amazon CloudWatch. Essa métrica pode ser visualizada na visualização de desempenho Outras métricas.

O AWS Management Pack também descobre os seguintes relacionamentos:

- AWS CloudFormation A pilha do e seus recursos do Elastic Load Balancing ou do Amazon EC2
- O load balancer do Elastic Load Balancing e suas instâncias do EC2
- A instância do Amazon EC2 e seus volumes do EBS
- A instância do Amazon EC2 e seu sistema operacional
- AWS Elastic BeanstalkO aplicativo do e seu ambiente, configuração e recursos

O AWS Management Pack descobre automaticamente a relação entre uma instância do EC2 e o sistema operacional que a executa. Para descobrir essa relação, o Operations Manager Agent deve ser instalado e configurado na instância, e o pacote de gerenciamento do sistema operacional correspondente deve ser importado no Operations Manager.

As descobertas são executadas nos servidores de gerenciamento no grupo de recursos (System Center 2012) ou no nó observador (System Center 2007 R2).

Descoberta	Intervalo (segundos)
Descoberta de recursos da Amazon (SCOM 2012)	14400
Descobre instâncias do EC2, volumes do Amazon EBS, load balancers e pilhas do CloudFront.	
AWS Elastic BeanstalkDescoberta do	14400
Descobre o AWS Elastic Beanstalk e sua relação com o ambiente, os recursos e a configuração.	
Descoberta de alarmes do CloudWatch	900
Descobre os alarmes gerados usando métricas do CloudWatch.	
Descoberta de métricas personalizadas do CloudWatch	14400
Descobre as métricas personalizadas do CloudWatch	
Descoberta de nó observador (SCOM 2007 R2)	14400
Tem como destino o servidor de gerenciamento raiz e cria os objetos do nó observador.	

Monitors

Monitores são usados para medir a integridade dos recursos da AWS. Os monitores executam nos servidores de gerenciamento no grupo de recursos (System Center 2012) ou no nó observador (System Center 2007 R2).

Monitor	Intervalo (segundos)
AWS CloudFormation Status de pilha do	900
Alarme de métrica do Amazon CloudWatch	300
Status do volume do Amazon EBS	900
Status de instância do Amazon EC2	900
Status do sistema de instância do Amazon EC2	900
AWS Elastic BeanstalkStatus do	900
Nó observador para a conectividade com a nuvem da Amazon (SCOM 2007 R2)	900

Rules

As regras criam alertas (com base nas métricas do Amazon CloudWatch) e coletam dados para análise e relatórios.

Rule	Intervalo (segundos)
AWSRegra de descoberta de recursos da (SCOM 2007 R2) Tem como destino o nó observador e usa a API da AWS para descobrir objetos para os seguintes recursos da AWS: instâncias do EC2, volumes do EBS,平衡adores de cargas e pilhas do AWS CloudFormation. (Métricas ou alarmes do CloudWatch não são descobertos). Após a descoberta ser concluída, visualize os objetos no estado Not Monitored (Não monitorado).	14400
Regra de coleta de dados das métricas de desempenho de volume do Amazon Elastic Block Store	900
Regra de coleta de dados das métricas de desempenho de instâncias do Amazon EC2	900
Regra de coleta de dados das métricas de desempenho do balanceamento do Elastic Load Balancing	900
Regra de coleta de dados de métrica personalizada do CloudWatch	900

Events

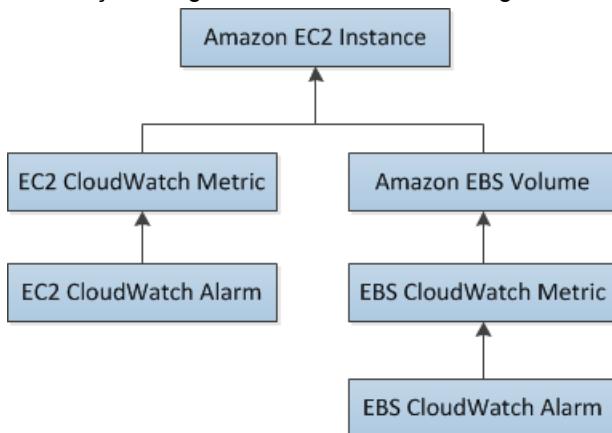
Relatório de eventos sobre atividades que envolvem recursos monitorados. Os eventos são gravados no log de eventos do Operations Manager.

ID do evento	Descrição
4101	Descoberta de instância do Amazon EC2 (descoberta geral) concluída
4102	Descoberta de métricas do Elastic Load Balancing Descoberta de métricas de volume do Amazon EBS,

ID do evento	Descrição
	Descoberta de métricas de instância do Amazon EC2 concluída
4103	Descoberta de alarmes de métricas do Amazon CloudWatch concluída
4104	Descoberta de computador Windows da Amazon concluída
4105	Coleta de alarmes de métricas da Amazon concluída
4106	Descoberta de relação de computador de instância do EC2 concluída
4107	Coleta de estado de pilha do AWS CloudFormation concluída
4108	Coleta de estado de disponibilidade de nó observador concluída
4109	Regra de coleta de métricas da Amazon concluída
4110	Tarefa de alteração de estado de instância da Amazon concluída
4111	Estado de monitor de status de instância do EC2 concluído
4112	Estado de monitor de status de volume do Amazon EBS concluído
4113	Estado de monitor de eventos programados de instância do Amazon EC2 calculado
4114	Estado de monitor de eventos programados do Amazon EBS calculado
4115	Descoberta do Elastic Beanstalk concluída
4116	Estado de status do ambiente do Elastic Beanstalk calculado
4117	Estado operacional do ambiente do Elastic Beanstalk calculado
4118	Estado da configuração do ambiente do Elastic Beanstalk calculado

Modelo de integridade

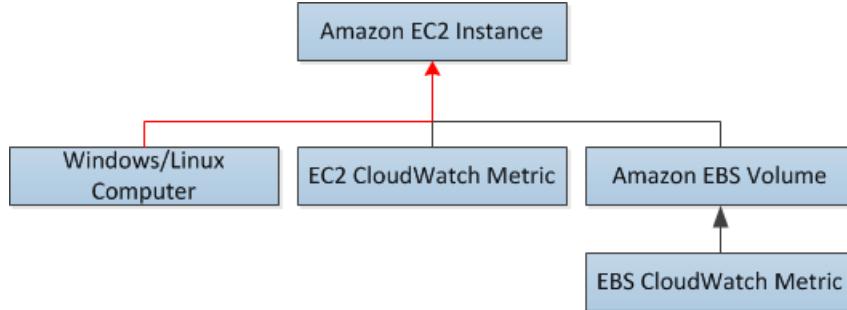
A ilustração a seguir mostra o modelo de integridade definido pelo AWS Management Pack.



O estado de integridade de um alarme do CloudWatch é acumulado para sua métrica correspondente do CloudWatch. O estado de integridade de uma métrica do CloudWatch para o Amazon EC2 é acumulado para a instância do EC2. De forma semelhante, o estado de integridade da métrica do CloudWatch para

o Amazon EBS é acumulado para o volume do Amazon EBS. Os estados de integridade de volumes do Amazon EBS volumes usados por uma instância do EC2 são acumulados para a instância do EC2.

Quando a relação entre uma instância do EC2 e o sistema operacional foi descoberta, o estado de integridade do sistema operacional é acumulado para a instância do EC2.

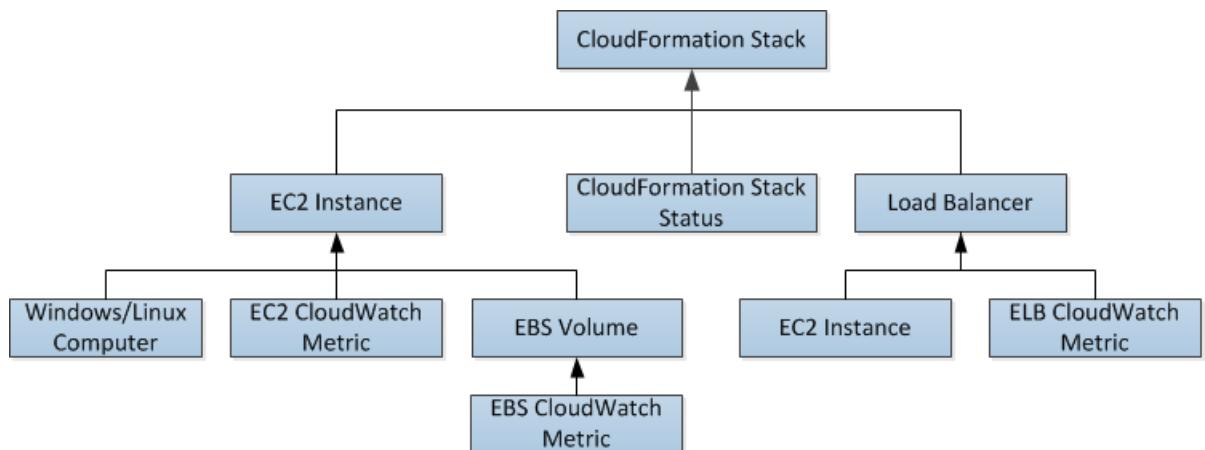


O estado de integridade de uma pilha do AWS CloudFormation depende do status da própria pilha do AWS CloudFormation e dos estados de integridade de seus recursos, especificamente load balancers e instâncias do EC2.

A tabela a seguir ilustra como o status da pilha do AWS CloudFormation corresponde a seu estado de integridade.

Estado de integridade	AWS CloudFormationStatus de pilha do	Observações
Erro	CREATE_FAILED DELETE_IN_PROGRESS DELETE_FAILED UPDATE_ROLLBACK_FAILED	Mais provavelmente utilizável
Aviso	UPDATE_ROLLBACK_IN_PROGRESS UPDATE_ROLLBACK_COMPLETE_CLEANUP_IN_PROGRESS UPDATE_ROLLBACK_COMPLETE	Recuperação após um problema
Integridade	CREATE_COMPLETE UPDATE_IN_PROGRESS UPDATE_COMPLETE_CLEANUP_IN_PROGRESS UPDATE_COMPLETE	Utilizável

O modelo de integridade completo para uma pilha do AWS CloudFormation é da seguinte forma:



Personalizar o AWS Management Pack

Para alterar a frequência das descobertas, regras e monitores, você pode substituir o tempo do intervalo (em segundos).

Para alterar a frequência

1. Na barra de ferramentas do Operations Manager (Gerenciador de operações), clique em Go (Acessar) e, em seguida, clique em Authoring (Criação).
2. No painel Authoring (Criação), expanda Management Pack Objects (Objetos do pacote de gerenciamento) e clique no objeto a ser alterado (por exemplo, Object Discoveries (Descobertas de objetos), Rules (Regras) ou Monitors (Monitores)).
3. Na barra de ferramentas, clique em Scope (Escopo).
4. Na caixa de diálogo Scope Management Pack Objects (Definir escopo dos objetos do pacote de gerenciamento), clique em View all targets (Visualizar todos os destinos).
5. Para limitar o escopo para objetos da Amazon, digite Amazon no campo Look for (Procurar por).
6. Selecione o objeto a ser configurado e clique em OK.
7. No painel central do Operations Manager (Gerenciador de operações), clique com o botão direito do mouse no objeto a ser configurado, clique em Overrides (Substituições) e, em seguida, clique no tipo de substituição que você deseja configurar.
8. Use a caixa de diálogo Override Properties (Propriedades de substituição) para definir valores e configurações diferentes para os objetos.

Tip

Para desabilitar uma descoberta, uma regra ou um objeto de monitoramento, clique com o botão direito do mouse no objeto a ser desabilitado no painel central do Operations Manager (Gerenciador de operações), clique em Overrides (Substituições) e, em seguida, clique em Disable the Rule (Desabilitar a regra). Você pode desabilitar regras se, por exemplo, você não executar aplicações do AWS Elastic Beanstalk ou usar métricas personalizadas do Amazon CloudWatch.

Para obter informações sobre como criar substituições, consulte [Como ajustar o monitoramento usando destinos e substituições](#) no site Microsoft TechNet.

Para obter informações sobre como criar regras e monitores, consulte [Criação do System Center 2012 – Operations Manager](#) ou o [Guia de criação do System Center Operations Manager 2007 R2 Management Pack](#) no site Microsoft TechNet.

Atualizar o AWS Management Pack

O procedimento que você usa para atualizar o AWS Management Pack depende da versão do System Center.

System Center 2012

Para atualizar o AWS Management Pack

1. No site [Suplementos da AWS para o Microsoft System Center](#), clique em SCOM 2012. Faça download do `AWS-SCOM-MP-2.0-2.5.zip` no computador e descompacte-o. O arquivo `.zip` inclui o `Amazon.AmazonWebServices.mpb`.
2. No console de operações, no menu Go (Acessar), clique em Administration (Administração) e, em seguida, clique em Management Packs (Pacotes de gerenciamento).
3. No painel Tasks (Tarefas), clique em Import Management Packs (Importar pacotes de gerenciamento).
4. Na página Select Management Packs (Selecionar pacotes de gerenciamento), clique em Add (Adicionar) e, em seguida, clique em Add from disk (Adicionar do disco).
5. Na caixa de diálogo Select Management Packs to import (Selecionar pacotes de gerenciamento para importar), selecione o arquivo `Amazon.AmazonWebServices.mpb` no local onde foi feito download e, em seguida, clique em Open (Abrir).
6. Na página Select Management Packs (Selecionar pacotes de gerenciamento), sob Import list (Importar lista), selecione o pacote de gerenciamento da Amazon Web Services e clique em Install (Instalar).

Se o botão **Install (Instalar)** estiver desabilitado, a atualização para a versão atual não será compatível e você deverá desinstalar o AWS Management Pack para poder instalar a versão atual. Para obter mais informações, consulte [Desinstalar o AWS Management Pack \(p. 1698\)](#).

System Center 2007 R2

Para atualizar o AWS Management Pack

1. No Servidor de gerenciamento, acesse o site [Suplementos da AWS para o Microsoft System Center](#) e clique em SCOM 2007. Salve o `AWS-MP-Setup-2.5.msi` e execute-o.
2. Clique em Next (Avançar) e siga as instruções para atualizar os componentes que você instalou anteriormente.
3. Se o servidor de gerenciamento raiz, o console de Operações e o nó observador estiverem em computadores diferentes, você deverá fazer download e executar o programa de configuração em cada computador.
4. No nó observador, abra uma janela de prompt de comando como administrador e execute os seguintes comandos.

```
C:\> net stop HealthService
The System Center Management service is stopping.
The System Center Management service was stopped successfully.

C:\> net start HealthService
The System Center Management service is starting.
The System Center Management service was started successfully.
```

5. No console de operações, no menu Go (Acessar), clique em Administration (Administração) e, em seguida, clique em Management Packs (Pacotes de gerenciamento).
6. No painel Actions (Ações), clique em Import Management Packs (Importar pacotes de gerenciamento).

7. Na página Select Management Packs (Selecionar pacotes de gerenciamento), clique em Add (Adicionar) e, em seguida, clique em Add from disk (Adicionar do disco).
8. Na caixa de diálogo Select Management Packs to import (Selecionar pacotes de gerenciamento para importar), altere o diretório para C:\Program Files (x86)\Amazon Web Services Management Pack, selecione o arquivo Amazon.AmazonWebServices.mp e, em seguida, clique em Open (Abrir).
9. Na página Select Management Packs (Selecionar pacotes de gerenciamento), sob Import list (Importar lista), selecione o pacote de gerenciamento da Amazon Web Services e clique em Install (Instalar).

Se o botão Install (Instalar) estiver desabilitado, a atualização para a versão atual não será compatível e você deverá desinstalar o AWS Management Pack primeiro. Para obter mais informações, consulte [Desinstalar o AWS Management Pack \(p. 1698\)](#).

Desinstalar o AWS Management Pack

Se você precisar desinstalar o AWS Management Pack, use o procedimento a seguir.

System Center 2012

Para desinstalar o AWS Management Pack

1. No console de operações, no menu Go (Acessar), clique em Administration (Administração) e, em seguida, clique em Management Packs (Pacotes de gerenciamento).
2. Clique com o botão direito do mouse em Amazon Web Services e selecione Delete (Excluir).
3. Na caixa de diálogo Dependent Management Packs (Pacotes de gerenciamento dependentes), anote quais são os pacotes de gerenciamento dependentes e clique em Close (Fechar).
4. Clique com o botão direito do mouse no pacote de gerenciamento e selecione Delete (Excluir).
5. Clique com o botão direito do mouse em Amazon Web Services e selecione Delete (Excluir).

System Center 2007 R2

Para desinstalar o AWS Management Pack

1. Conclua as etapas 1 a 5 descritas para o System Center 2012 na seção anterior.
2. No Painel de Controle, abra Programas e Recursos. Selecione Amazon Web Services Management Pack (Pacote de gerenciamento da Amazon Web Services) e clique em Uninstall (Desinstalar).
3. Se o servidor de gerenciamento raiz, o console de Operações e o nó observador estiverem em computadores diferentes, você deverá repetir esse processo em cada computador.

Solucionar problemas do AWS Management Pack

Os seguintes são erros comuns, eventos e etapas de solução de problemas.

Tópicos

- [Erros 4101 e 4105 \(p. 1699\)](#)
- [Erro 4513 \(p. 1699\)](#)
- [Evento 623 \(p. 1699\)](#)

- [Eventos 2023 e 2120 \(p. 1699\)](#)
- [Evento 6024 \(p. 1700\)](#)
- [Solução de problemas em geral do System Center 2012 — Operations Manager \(p. 1700\)](#)
- [Solução de problemas em geral para o System Center 2007 R2 \(p. 1701\)](#)

Erros 4101 e 4105

Se receber um dos seguintes erros, você deverá atualizar o AWS Management Pack. Para obter mais informações, consulte [Atualizar o AWS Management Pack \(p. 1697\)](#).

```
Error 4101
Exception calling "DescribeVolumes" with "1" argument(s): "AWS was not able to validate
the
provided access credentials"
```

```
Error 4105
Exception calling "DescribeApplications" with "0" argument(s): "The security token
included
in the request is invalid"
```

Erro 4513

Se receber um dos seguintes erros, você deverá atualizar o AWS Management Pack. Para obter mais informações, consulte [Atualizar o AWS Management Pack \(p. 1697\)](#).

```
Error 4513
The callback method DeliverDataToModule failed with exception "Resolution of the
dependency
failed, type = "Amazon.SCOM.SDK.Interfaces.IMonitorSdk", name = "(none)".
Exception occurred while: Calling constructor Amazon.SCOM.SDK.CloudWatch.AwsMonitorSdk
(System.String awsAccessKey, System.String awsSecretKey).
Exception is: InvalidOperationException - Collection was modified; enumeration operation
may not run.
```

Evento 623

Se você encontrar o evento a seguir no log de eventos do Windows, siga a solução descrita em [KB975057](#).

```
Event ID: 623
HealthService (process_id) The version store for instance instance ("name") has reached
its maximum size of size MB. It is likely that a long-running transaction is preventing
cleanup of the version store and causing it to build up in size. Updates will be rejected
until the long-running transaction has been completely committed or rolled back.
Possible long-running transaction:
SessionId: id
Session-context: value
Session-context ThreadId: id
Cleanup: value
```

Eventos 2023 e 2120

Se você encontrar os seguintes eventos no log de eventos do Windows, consulte [IDs de eventos 2023 e 2120](#) para obter mais informações.

```
Event ID: 2023
The Health Service has removed some items from the send queue for management group
"Servers"
since it exceeded the maximum allowed size of size megabytes.
```

```
Event ID: 2120
The Health Service has deleted one or more items for management group "Servers" which
could
not be sent in 1440 minutes.
```

Evento 6024

Se você encontrar o seguinte evento no log de eventos do Windows, consulte [SCOM 2012 - ID do evento 6024](#) para obter mais informações.

```
Event ID: 6024
LaunchRestartHealthService.js : Launching Restart Health Service. Health Service exceeded
Process\Handle Count or Private Bytes threshold.
```

Solução de problemas em geral do System Center 2012 — Operations Manager

Tente o seguinte para resolver qualquer problema.

- Verifique se você instalou o pacote cumulativo de atualizações para o System Center 2012 — Operations Manager. O AWS Management Pack exige pelo menos o pacote cumulativo de atualizações 1.
- Verifique se você configurou o AWS Management Pack depois de importá-lo executando o Assistente de adição de monitoramento. Para obter mais informações, consulte [Etapa 1: Instalar o AWS Management Pack \(p. 1666\)](#).
- Verifique se você esperou o tempo suficiente para os recursos da AWS serem descobertos (10 a 20 minutos).
- Verifique se os servidores de gerenciamento estão configurados corretamente.
 - Os servidores de gerenciamento devem ter conectividade com a Internet.
 - A conta de ação para um servidor de gerenciamento deve ter privilégios de administrador local no servidor de gerenciamento.
 - O servidor de gerenciamento deve ter o .NET Framework 4.5. ou posterior.
- Verifique se a conta Executar como da AWS é válida.
 - Os valores para o ID da chave de acesso e a chave de acesso secreta estão corretos.
 - As chaves de acesso estão ativas: no AWS Management Console, clique em seu nome na barra de navegação e clique em Security Credentials (Credenciais de segurança).
 - O usuário do IAM tem pelo menos permissão de acesso somente leitura. Observe que o acesso somente leitura permite ao usuário ações que não alteram o estado de um recurso, como monitoramento, mas não permite ações de usuário como executar ou parar uma instância.
 - Se uma métrica do Amazon CloudWatch for mostrada como Not Monitored (Não monitorado), verifique se pelo menos um alarme do Amazon CloudWatch foi definido para essa métrica do Amazon CloudWatch.
 - Para soluções de problemas adicionais, use as informações nos logs de eventos.
 - Verifique o log de eventos do Operations Manager no servidor de gerenciamento. Para obter mais informações, consulte [Events \(p. 1693\)](#) para obter uma lista de eventos que o AWS Management Pack grava no log de eventos do Operations Manager.

Solução de problemas em geral para o System Center 2007 R2

Tente o seguinte para resolver qualquer problema.

- Verifique se você configurou o AWS Management Pack depois de importá-lo executando o Assistente de adição de monitoramento. Para obter mais informações, consulte [Etapa 1: Instalar o AWS Management Pack \(p. 1666\)](#).
- Verifique se você esperou o tempo suficiente para os recursos da AWS serem descobertos (10 a 20 minutos).
- Verifique se o nó observador está configurado corretamente.
 - O agente de proxy está habilitado. Para obter mais informações, consulte [Etapa 2: Configurar o nó observador \(p. 1667\)](#).
 - O nó observador tem conectividade com a Internet.
 - A conta de ação do nó observador tem privilégios de administrador local no nó observador.
 - O nó observador deve ter o .NET Framework 3.5.1. ou posterior.
- Verifique se o nó observador está íntegro e resolva todos os alertas. Para obter mais informações, consulte [Views \(p. 1677\)](#).
- Verifique se a conta Executar como da AWS é válida.
 - Os valores para o ID da chave de acesso e a chave de acesso secreta estão corretos.
 - As chaves de acesso estão ativas: no AWS Management Console, clique em seu nome na barra de navegação e clique em Security Credentials (Credenciais de segurança).
 - O usuário do IAM tem pelo menos permissão de acesso somente leitura. Observe que o acesso somente leitura permite ao usuário ações que não alteram o estado de um recurso, como monitoramento, mas não permite ações de usuário como executar ou parar uma instância.
 - Se uma métrica do Amazon CloudWatch for mostrada como Not Monitored (Não monitorado), verifique se pelo menos um alarme do Amazon CloudWatch foi definido para essa métrica do Amazon CloudWatch.
 - Para soluções de problemas adicionais, use as informações nos logs de eventos.
 - Verifique o log de eventos do Operations Manager no servidor de gerenciamento e no nó observador. Para obter mais informações, consulte [Events \(p. 1693\)](#) para obter uma lista de eventos que o AWS Management Pack grava no log de eventos do Operations Manager.

Informações relacionadas

Os recursos relacionados a seguir podem ajudar você à medida que trabalha com este serviço.

Windows na AWS

- [Windows naAWS](#): visão geral do Windows em workloads e produtos da AWS.
- [Amazon Web Services e Microsoft: Perguntas frequentes](#): Perguntas frequentes específicas para executar o software da Microsoft na AWS.
- [Licenciar Microsoft na AWS: Opções para usar licenças de software da Microsoft na Nuvem AWS – Opções para usar licenças de software da Microsoft na Nuvem AWS](#) – Opções para usar licenças de software da Microsoft na Nuvem AWS.
- [AWSMigration Acceleration Program para Windows](#): produtos, práticas recomendadas e ferramentas da AWS para ajudar você a economizar e acelerar as migrações de workloads do Windows para a AWS.
- [AWSOptimization and Licensing Assessment](#): avalie seu ambiente Windows para reduzir custos e otimizar a computação.
- [EC2 Image Builder](#): automatize a criação, o gerenciamento e a implantação de imagens de servidor personalizadas, seguras e atualizadas que são pré-instaladas e pré-configuradas com configurações de software para atender a padrões específicos de TI.
- [AWS Launch Wizard](#): o AWS Launch Wizard orienta você durante o dimensionamento, a configuração e a implantação de aplicações na AWS seguindo o AWS Well-Architected Framework.
- [Microsoft SQL Server na AWS](#): visão geral do Microsoft SQL Server em workloads e produtos da AWS.

Forum

[Fórum do Amazon EC2](#): fórum de discussão da AWS referente ao Amazon EC2 para publicar perguntas e comentários.

Pricing

[Definição de preço do Amazon EC2](#): informações sobre definição de preço para o Amazon EC2.

Tutorials

[Tutoriais práticos](#): comece a usar tutoriais passo a passo para iniciar sua primeira aplicação.

Recursos gerais da AWS

Os seguintes recursos relacionados podem ajudá-lo enquanto você trabalha com o AWS.

- [Aulas e workshops](#): links para cursos de especialidades e baseados em função, além de laboratórios autoguiados para ajudar a aperfeiçoar suas habilidades na AWS e a obter experiência prática.
- [Ferramentas do desenvolvedor da AWS](#): links para ferramentas de desenvolvedor, SDKs, toolkits de IDE e ferramentas da linha de comando para desenvolver e gerenciar aplicações da AWS.
- [Whitepapers da AWS](#): links para uma lista abrangente de whitepapers técnicos da AWS que abrangem tópicos, como arquitetura, segurança e economia, elaborados pelos arquitetos de soluções da AWS ou por outros especialistas técnicos.
- [AWS Support Center](#): o centro para criar e gerenciar os seus casos da AWS Support. Também inclui links para outros recursos úteis, como fóruns, perguntas frequentes técnicas, status de integridade do serviço e AWS Trusted Advisor.

- [AWS Support](#): a página Web principal para obter informações sobre o AWS Support, um canal de suporte de resposta rápida e com atendimento individual para ajudar a construir e a executar aplicações na nuvem.
- [Entre em contato conosco](#): um ponto central de contato para consultas relativas a faturamento, conta, eventos, abuso e outros problemas da AWS.
- [AWSTermos do site da](#) : informações detalhadas sobre os nossos direitos autorais e marca registrada. Sua conta, licença e acesso ao site, entre outros tópicos.

Histórico do documento

A tabela a seguir descreve adições importantes na documentação do Amazon EC2 desde 2019. Também atualizamos a documentação com frequência para abordar os comentários enviados por você.

update-history-change	atualização da descrição do histórico	atualização da data do histórico
Reservas de Capacidade sob demanda e direcionadas para EC2 Fleet	O EC2 Fleet pode iniciar Instâncias sob demanda nas Reservas de Capacidade targeted .	22 de setembro de 2021
Instâncias T3 em Hosts Dedicados	Support para instâncias T3 no Host Dedicado Amazon EC2.	14 de setembro de 2021
Suporte de hibernação para RHEL, Fedora e CentOS	Coloque em hibernação suas instâncias recém-iniciadas que foram iniciadas a partir de AMIs RHEL, Fedora e CentOS.	9 de setembro de 2021
Novas Local Zones adicionadas	Adicionar Local Zones em Chicago, Minneapolis e Kansas City.	8 de setembro de 2021
Amazon EC2 Global View	O Amazon EC2 Global View permite que você visualize VPCs, sub-redes, instâncias, grupos de segurança e volumes em várias Regiões do AWS em um único console.	1º de setembro de 2021
Suporte de defasagem de AMI para Amazon Data Lifecycle Manager	As políticas de AMI apoiadas pelo EBS do Amazon Data Lifecycle Manager podem defasar AMIs. A política gerenciada do AWS <code>AWSDataLifecycleManagerServiceRoleForManagement</code> foi atualizada para ser compatível com esse recurso.	23 de agosto de 2021
Suporte à hibernação para C5d, M5d e R5d	Coloque em hibernação suas instâncias recém-iniciadas em execução nos tipos de instância C5d, M5d e R5d.	19 de agosto de 2021
Pares de chave do Amazon EC2	O Amazon EC2 agora é compatível com chaves ED25519 em instâncias Linux e Mac.	17 de agosto de 2021
Instâncias M6i (p. 1704)	Novas instâncias de uso geral com processadores Intel Xeon escalável de terceira geração (Ice Lake).	16 de agosto de 2021

Métricas do CloudWatch para o Amazon Data Lifecycle Manager	É possível monitorar suas políticas do Amazon Data Lifecycle Manager usando o Amazon CloudWatch.	28 de julho de 2021
Nova Local Zone adicionada	Adicionar Local Zone em Denver.	27 de julho de 2021
Eventos de dados do CloudTrail para APIs diretas do EBS	As APIs ListSnapshotBlocks, ListChangedBlocks, GetSnapshotBlock e PutSnapshotBlock podem ser eventos de dados registrados no CloudTrail.	27 de julho de 2021
Prefixos para interfaces de rede	É possível atribuir um intervalo de CIDR IPv4 ou IPv6 privado, de modo automático ou manual, às interfaces de rede.	22 de julho de 2021
Volumes io2 do Block Express	Os volumes io2 Block Express agora estão disponíveis ao público em geral em todas as regiões e zonas de disponibilidade com suporte para instâncias R5b.	19 de julho de 2021
Janelas de eventos	Você pode definir janelas de eventos personalizadas e semanais para eventos programados que reinicializam, interrompem ou terminam suas instâncias do Amazon EC2.	15 de julho de 2021
IDs de recursos e suporte a marcação para regras de grupo de segurança (p. 1704)	Você pode fazer referência a regras de grupo de segurança por ID de recurso. Você também pode adicionar tags a regras de grupos de segurança.	7 de julho de 2021
Novas Local Zones adicionadas	Adicionar Local Zones em Dallas e na Filadélfia.	7 de julho de 2021
Defasar uma AMI	Agora você pode especificar quando uma AMI é defasada.	11 de junho de 2021
Cobrança do Windows por segundo (p. 1704)	O Amazon EC2 cobra por segundo pela utilização baseada em Windows e SQL Server, com cobrança mínima de um minuto.	10 de junho de 2021
Reservas de Capacidade no AWS Outposts	Agora você pode usar as Reservas de Capacidade no AWS Outposts.	24 de maio de 2021
Compartilhamento de reserva de capacidade	Agora é possível compartilhar Reservas de Capacidade criadas em Local Zones e zonas do Wavelength.	24 de maio de 2021

Instâncias virtualizadas com mais memória (p. 1704)	Instâncias com mais memória virtualizadas criadas especificamente para executar grandes bancos de dados na memória. Os novos tipos são u-6tb1.56xlarge, u-6tb1.112xlarge, u-9tb1.112xlarge e u-12tb1.112xlarge.	11 de maio de 2021
Substituição do volume raiz	Agora você pode usar tarefas de substituição de volume raiz para substituir o volume raiz do EBS para instâncias em execução.	22 de abril de 2021
Armazenar e restaurar uma AMI usando o S3	Armazene AMIs baseadas em EBS no S3 e restaure-as a partir do S3 para permitir a cópia de AMIs entre partições.	6 de abril de 2021
Console serial do EC2	Solucionar problemas de inicialização e conectividade de rede estabelecendo uma conexão com a porta serial de uma instância.	30 de março de 2021
Modos de inicialização	O Amazon EC2 agora é compatível com a inicialização UEFI em determinadas instâncias do EC2 baseadas em AMD e Intel.	22 de março de 2021
Amazon EBS local snapshots on Outposts	Agora você pode usar Snapshots locais do Amazon EBS em Outposts da Amazon para armazenar snapshots de volumes em um Outpost localmente no Amazon S3 no próprio Outpost.	4 de fevereiro de 2021
Crie um registro de DNS reverso	Agora você pode configurar a pesquisa de DNS reverso para os seus endereços IP elásticos.	3 de fevereiro de 2021
Amazon Data Lifecycle Manager	Use o Amazon Data Lifecycle Manager para automatizar o processo de compartilhamento de snapshots e copiá-los em todas as contas da AWS.	17 de dezembro de 2020
Instâncias do G4ad (p. 1704)	Novas instâncias alimentadas por GPUs AMD Radeon Pro V520 e processadores AMD EPYC de 2ª geração.	9 de dezembro de 2020
Marcar AMIs e snapshots na criação de AMI	Ao criar uma AMI, você pode marcar a AMI e os snapshots com as mesmas tags, ou pode marcá-los com tags diferentes.	4 de dezembro de 2020

Visualização de io2 Block Express	Agora você pode optar por participar da demonstração de volumes io2 Block Express. io2 Os volumes Block Express fornecem latência abaixo de um milissegundo e oferece suporte a IOPS maiores, maior taxa de transferência e maior capacidade que os volumes io2.	1º de dezembro de 2020
volumes gp (p. 1704)	Um novo tipo de volume de Finalidade geral (SSD) do Amazon EBS. Você pode especificar IOPS provisionadas e taxa de transferência ao criar ou modificar o volume.	1º de dezembro de 2020
Instâncias D3, D3en, M5zn e R5b (p. 1704)	Novos tipos de instância criados no sistema Nitro.	1º de dezembro de 2020
Tamanhos de volume de disco rígido otimizado e disco rígido frio com taxa de transferência	Os volumes de disco rígido (st1) Optimized Throughput (Taxa de transferência otimizada) (sc1) e disco rígido frio podem variar em tamanho de 125 GiB a 16 TiB.	30 de novembro de 2020
Use o Amazon EventBridge para monitorar eventos de frota spot	Crie regras do EventBridge que açãoem ações programáticas em resposta a alterações e erros de estado de frota spot.	20 de novembro de 2020
Use Amazon EventBridge para monitorar eventos de Frota do EC2	Crie regras de EventBridge que açãoem ações programáticas em resposta a alterações e erros de estado de Frota do EC2.	20 de novembro de 2020
Excluir frotas de instant	Exclua uma Frota do EC2 do tipo instant e encerre todas as instâncias na frota em uma única chamada de API.	18 de novembro de 2020
Suporte de hibernação para T3 e T3a	Hiberne suas instâncias recém-executadas em execução em tipos de instância T3 e T3a.	17 de novembro de 2020
Amazon Data Lifecycle Manager	Você pode usar o Amazon Data Lifecycle Manager para automatizar a criação, a retenção e a exclusão de AMIs suportadas pelo EBS.	9 de novembro de 2020
Categoria de metadados da instância: eventos/recomendações/rebalanceamento	O tempo aproximado, em UTC, quando a notificação de recomendação de rebalanceamento da instância do EC2 é emitida para a instância.	4 de novembro de 2020

Recomendação de rebalanceamento de instâncias do EC2	Um sinal que o notifica quando uma instância spot está em risco elevado de interrupção.	4 de novembro de 2020
Reservas de Capacidade em zonas Wavelength	Reservas de Capacidade agora podem ser criadas e usadas em zonas Wavelength.	4 de novembro de 2020
Rebalanceamento de capacidade	Configure a frota spot ou a EC2 Fleet para executar uma instância spot de substituição quando o Amazon EC2 emitir uma recomendação de rebalanceamento.	4 de novembro de 2020
Suporte à hibernação para I3, M5ad e R5ad	Hibernar suas instâncias recém-iniciadas em execução nos tipos de instância I3, M5ad e R5ad.	21 de outubro de 2020
Limites de vCPU da instância spot	Os limites da instância spot agora são gerenciados em termos do número de vCPUs que suas instâncias spot em execução estão usando ou usarão até o atendimento de solicitações abertas.	1º de outubro de 2020
Reservas de Capacidade em Local Zones	Reservas de Capacidade agora podem ser criadas e usadas em Local Zones.	30 de setembro de 2020
Amazon Data Lifecycle Manager	As políticas do Amazon Data Lifecycle Manager podem ser configuradas com até quatro programações.	17 de setembro de 2020
Suporte à hibernação para M5a e R5a	Hiberne suas instâncias recém-executadas em execução nos tipos de instância M5a e R5a.	28 de agosto de 2020
Volumes SSD de IOPS provisionadas (io2) para Amazon EBS	Volumes SSD de IOPS provisionadas (io2) são criados para fornecer 99,999% de durabilidade de volume com uma AFR até 0,001%.	24 de agosto de 2020
Os metadados da instância fornecem informações de posicionamento e localização da instância	Novos campos de metadados de instância na categoria placement: região, nome do placement group, número da partição, ID do host e ID da zona de disponibilidade.	24 de agosto de 2020
Instâncias C5ad (p. 1704)	Novas instâncias otimizadas para computação com processadores AMD EYPC de segunda geração.	13 de agosto de 2020

Zonas do Wavelength	Uma Wavelength Zone é uma zona isolada no local da transportadora em que a infraestrutura de Wavelength é implantada.	6 de agosto de 2020
Grupos de Reserva de capacidade	Você pode usar AWS Resource Groups para criar coleções lógicas de Reservas de Capacidade e, depois, direcionar execuções de instâncias nesses grupos.	29 de julho de 2020
Restauração rápida de snapshots	Você pode habilitar a restauração rápida de snapshots compartilhados com você.	21 de julho de 2020
EC2Launch v2 (p. 482)	Você pode usar o EC2Launch v2 para executar tarefas durante o startup da instância se uma instância for interrompida e iniciada posteriormente, se uma instância for reiniciada, e também sob demanda. O EC2Launch v2 é compatível com todas as versões do Windows Server e substitui o EC2Launch e o EC2Config.	30 de junho de 2020
Instâncias bare metal para G4dn (p. 1704)	Novas instâncias que fornecem aos aplicativos acesso direto aos recursos físicos do servidor de host.	5 de junho de 2020
Instâncias C5a (p. 1704)	Novas instâncias otimizadas para computação com processadores AMD EYPC de segunda geração.	4 de junho de 2020
Traga seus próprios endereços IPv	Você pode trazer parte ou todo o seu intervalo de endereços IPv6 da rede no local para sua conta da AWS.	21 de maio de 2020
Executar instâncias usando um parâmetro do Systems Manager	Você pode especificar um parâmetro do AWS Systems Manager em vez de uma AMI ao executar uma instância.	5 de maio de 2020
Personalizar notificações de eventos programados	É possível personalizar notificações de eventos programados para incluir tags na notificação por e-mail.	4 de maio de 2020
Windows Server no Hosts dedicados	Você pode usar as AMIs do Windows Server fornecidas pela Amazon para executar as versões mais recentes do Windows Server no Hosts dedicados.	7 de abril de 2020

Interromper e iniciar uma instância spot	Agora você pode interromper suas instâncias spot com base no Amazon EBS e iniciá-las à vontade, em vez de depender do comportamento de interrupção.	13 de janeiro de 2020
Marcação de recursos (p. 1704)	Você pode marcar gateways da Internet somente de saída, gateways locais, tabelas de rotas de gateway, interfaces virtuais de gateway locais, grupos de interface virtual de gateway local, associações de VPC da tabela de rotas do gateway local e associações de grupo de interface virtual da tabela de rotas do gateway local	10 de janeiro de 2020
Conectar-se à sua instância usando o Gerenciador de sessões	Você pode iniciar uma sessão do Gerenciador de sessões com uma instância no console do Amazon EC2.	18 de dezembro de 2019
Hosts dedicados e grupos de recursos de host	Hosts dedicados agora podem ser usados com grupos de recursos de host.	2 de dezembro de 2019
Compartilhamento de Host dedicado	Agora é possível compartilhar os hosts dedicados entre contas da AWS.	2 de dezembro de 2019
Especificação de crédito padrão no nível da conta	É possível definir a especificação de crédito padrão por família de instâncias expansíveis no nível da conta, por região da AWS.	25 de novembro de 2019
Descoberta de tipo de instância	Você pode encontrar um tipo de instância que atenda às suas necessidades.	22 de novembro de 2019
Dedicated Hosts (p. 1704)	Agora, é possível configurar um Host dedicado para oferecer suporte a vários tipos de instância em uma família de instâncias.	21 de novembro de 2019
Restaurações rápidas de snapshots do Amazon EBS	É possível habilitar restaurações rápidas de snapshots em um snapshot do EBS para garantir que os volumes do EBS criados a partir de um snapshot sejam totalmente inicializados na criação e entreguem instantaneamente toda a sua performance provisionada.	20 de novembro de 2019

Instance Metadata Service Version 2	É possível usar o Serviço de metadados da instância versão 2, que é um método orientado a sessão para solicitação de metadados da instância.	19 de novembro de 2019
Suporte para hibernação de instâncias do Windows sob demanda	Você pode hibernar instâncias do Windows sob demanda.	14 de outubro de 2019
Compras na fila de Instâncias reservadas	É possível colocar a compra de uma Instância reservada na fila até três anos de maneira antecipada.	4 de outubro de 2019
Instâncias do G4dn (p. 1704)	Novas instâncias com GPUs NVIDIA Tesla.	19 de setembro de 2019
Interrupção para diagnóstico	É possível enviar uma interrupção para diagnóstico a uma instância inacessível ou sem resposta a fim de acionar um erro de tela azul/interrupção.	14 de agosto de 2019
Estratégia de alocação otimizada por capacidade	Com o uso de EC2 Fleet ou de frota spot, agora é possível executar instâncias spot a partir de grupos spot com a capacidade ideal para o número de instâncias que estão sendo executadas.	12 de agosto de 2019
Compartilhamento do Reservas de capacidade sob demanda	Agora é possível compartilhar as Reservas de Capacidade entre contas da AWS.	29 de julho de 2019
Marcação de recursos (p. 1704)	Executar modelos na criação.	24 de julho de 2019
Recuperação do host	Reinic peace automaticamente suas instâncias em um novo host no caso de uma falha inesperada do hardware em um Host dedicado.	5 de junho de 2019
Snapshots de vários volumes do Amazon EBS	É possível tirar snapshots exatos de momentos específicos, coordenados por dados e consistentes com falhas em vários volumes do EBS associados a uma instância do EC2.	29 de maio de 2019
Marcação de recursos (p. 1704)	Você pode marcar Reservas de hosts dedicados.	27 de maio de 2019

Criptografia por padrão do Amazon EBS	Depois de habilitar a criptografia por padrão em uma região, todos os novos volumes do EBS que você criar nessa região serão criptografados usando a Chave do KMS padrão para criptografia do EBS.	23 de maio de 2019
Snapshots consistentes com aplicativo VSS	Crie snapshots consistentes com o aplicativo de todos os volumes do Amazon EBS anexados às instâncias do Windows usando o Run Command do AWS Systems Manager.	13 de maio de 2019
Marcação de recursos (p. 1704)	É possível marcar VPC endpoints, serviços de endpoint e configurações do serviço de endpoint.	13 de maio de 2019
Assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server	Mover workloads existentes do Microsoft SQL Server de um sistema operacional Windows para Linux.	8 de maio de 2019
Instâncias I3en (p. 1704)	As novas instâncias I3en podem utilizar até 100 Gbps de largura de banda de rede.	8 de maio de 2019
Atualização automatizada do Windows	Execute atualizações automatizadas de instâncias do EC2 do Windows usando o AWS Systems Manager.	6 de maio de 2019
Instâncias T3a (p. 1704)	Novas instâncias com processadores AMD EYPC.	24 de abril de 2019
Instâncias M5ad e R5ad (p. 1704)	Novas instâncias com processadores AMD EYPC.	27 de março de 2019
Marcação de recursos (p. 1704)	Você pode atribuir tags personalizadas às reservas de Host dedicado para categorizá-las de diferentes maneiras.	14 de março de 2019
Instâncias bare metal para M5, M5d, R5, R5d e z1d (p. 1704)	Novas instâncias que fornecem aos aplicativos acesso direto aos recursos físicos do servidor de host.	13 de fevereiro de 2019

História dos anos anteriores

A tabela a seguir descreve adições importantes na documentação do Amazon EC2 em 2018 e em anos anteriores.

Recurso	Versão da API	Descrição	Data de lançamento
Placement groups de partição	15/11/2016	Os placement groups de partição distribuem instâncias entre partições lógicas, garantindo que instâncias em uma partição não compartilhem hardware subjacente com instâncias em outras partições. Para obter mais informações, consulte Placement groups de partição (p. 1045) .	20 de dezembro de 2018
Instâncias p3dn.24xlarge	15/11/2016	As novas instâncias p3dn.24xlarge fornecem 100 Gbps de largura de banda de rede.	7 de dezembro de 2018
Instâncias com 100 Gbps de largura de banda de rede	15/11/2016	As novas instâncias C5n podem utilizar até 100 Gbps de largura de banda de rede.	26 de novembro de 2018
O console do Spot recomenda uma frota de instâncias	15/11/2016	O console do Spot recomenda uma frota de instâncias com base na melhor prática do Spot (diversificação de instâncias) para atender às especificações mínimas de hardware (vCPUs, memória e armazenamento) para a necessidade de sua aplicação. Para obter mais informações, consulte Criar uma solicitação de frota spot (p. 776) .	20 de novembro de 2018
Novo tipo de solicitação de Frota do EC2: instant	15/11/2016	Agora, o Frota do EC2 oferece suporte a um novo tipo de solicitação, instant, que pode ser usada para provisionar capacidade de forma síncrona entre tipos de instâncias e modelos de compra. A solicitação instant retorna as instâncias executadas na resposta da API e não toma nenhuma ação adicional permitindo que você controle se e quando as instâncias são executadas. Para obter mais informações, consulte Tipos de solicitação da Frota do EC2 (p. 714) .	14 de novembro de 2018
Instâncias com processadores AMD EYPC	15/11/2016	As novas instâncias de uso geral (M5a) e de memória otimizada (R5a) oferecem opções de preços mais baixos para microsserviços, bancos de dados pequenos a médios, desktops virtuais, ambientes de desenvolvimento e teste, aplicações de negócios e muito mais.	6 de novembro de 2018
Informações sobre economias do Spot	15/11/2016	Você pode visualizar as economias feitas com o uso de instâncias spot para uma única frota spot ou para todas as instâncias spot. Para obter mais informações, consulte Economia na compra das Instâncias spot (p. 307) .	5 de novembro de 2018
Suporte do console para otimização de opções de CPU	15/11/2016	Ao executar uma instância, você pode otimizar as opções de CPU para atender a workloads ou necessidades de negócios específicas usando o console do Amazon EC2. Para obter mais informações, consulte Otimizar as opções de CPU (p. 582) .	31 de outubro de 2018

Recurso	Versão da API	Descrição	Data de lançamento
Suporte do console para criação de um modelo de execução usando uma instância	15/11/2016	Você pode criar um modelo de execução usando uma instância como a base para um novo modelo de execução usando o console do Amazon EC2. Para obter mais informações, consulte Criar um modelo de execução (p. 427) .	30 de outubro de 2018
On-Demand Capacity Reservations	15/11/2016	Você pode reservar capacidade para suas instâncias do Amazon EC2 em uma zona de disponibilidade específica por qualquer duração. Isso permite criar e gerenciar Reservas de Capacidade de forma independente dos descontos de faturamento oferecidos pelas Instâncias reservadas (RI - Reserved instances). Para obter mais informações, consulte On-Demand Capacity Reservations (p. 390) .	25 de outubro de 2018
Traga seus próprios endereços IP (BYOIP)	15/11/2016	Você pode trazer parte ou todo o seu intervalo de endereços IPv4 públicos da rede local para sua conta da AWS. Depois de levar o intervalo de endereços para a AWS, ele aparece em sua conta como um grupo de endereços. Você pode criar um endereço IP elástico de seu grupo de endereços e usá-lo com seus recursos da AWS. Para obter mais informações, consulte Traga seus próprios endereços IP (BYOIP) no Amazon EC2 (p. 972) .	23 de outubro de 2018
Instâncias g3s.xlarge	15/11/2016	Expande o intervalo da família de instâncias G3 de computação acelerada com a introdução de instâncias g3s.xlarge.	11 de outubro de 2018
Tag de Host dedicado na criação e suporte do console	15/11/2016	Você pode marcar seus Hosts dedicados na criação e gerenciar as tags de Host dedicado usando o console do Amazon EC2. Para obter mais informações, consulte Alocar Hosts dedicados (p. 355) .	08 de outubro de 2018
Instâncias com mais memória	15/11/2016	Essas instâncias são criadas especificamente para executar grandes bancos de dados na memória. Eles oferecem performance bare metal com acesso direto ao hardware do host. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 211) .	27 de setembro de 2018
Instâncias f1.4xlarge	15/11/2016	Expande o intervalo da família de instâncias F1 de computação acelerada com a introdução de instâncias f1.4xlarge.	25 de setembro de 2018
Suporte ao console para escalabilidade programada para a frota spot	15/11/2016	Aumentar ou diminuir a capacidade atual da frota com base em data e hora. Para obter mais informações, consulte Alterar a escala da frota spot usando a escalabilidade programada (p. 797) .	20 de setembro de 2018

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias T3	15/11/2016	As instâncias T3 são um tipo de instância de uso geral com capacidade de intermitência que fornecem um nível de linha de base de performance de CPU com a capacidade de intermitência para uso de CPU a qualquer momento e pelo tempo necessário. Para obter mais informações, consulte Instâncias expansíveis (p. 169) .	21 de agosto de 2018
Estratégias de alocação para Frotas do EC2	15/11/2016	Você pode especificar se a capacidade sob demanda é atendida pelo preço (preço mais baixo primeiro) ou prioridade (prioridade mais alta primeiro). Você pode especificar o número de grupos spot para os quais alocar sua capacidade spot de destino. Para obter mais informações, consulte Estratégias de alocação para Instâncias spot (p. 733) .	26 de julho de 2018
Estratégias de alocação para Frotas spot	15/11/2016	Você pode especificar se a capacidade sob demanda é atendida pelo preço (preço mais baixo primeiro) ou prioridade (prioridade mais alta primeiro). Você pode especificar o número de grupos spot para os quais alocar sua capacidade spot de destino. Para obter mais informações, consulte Estratégia de alocação para Instâncias spot (p. 762) .	26 de julho de 2018
Instâncias R5 e R5d	15/11/2016	As instâncias R5 e R5d são ideais para bancos de dados de alta performance, caches na memória distribuídos e análises na memória. As instâncias R5d vêm com volumes de armazenamento de instâncias do NVMe. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 211) .	25 de julho de 2018
Instâncias z1d	15/11/2016	Essas instâncias são projetadas para aplicações que exigem alta performance por núcleo com uma grande quantidade de memória, como a Electronic Design Automation (EDA) e bancos de dados relacionais. Essas instâncias vêm com volumes de armazenamento de instâncias do NVMe. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 211) .	25 de julho de 2018
Automação do ciclo de vida do snapshot	15/11/2016	Você pode usar o Amazon Data Lifecycle Manager para automatizar a criação e a exclusão de snapshots para seus volumes do EBS. Para obter mais informações, consulte Amazon Data Lifecycle Manager (p. 1363) .	12 de julho de 2018

Recurso	Versão da API	Descrição	Data de lançamento
Opções de CPU em modelos de execução	15/11/2016	Quando você cria um modelo de execução usando as ferramentas de linha de comando, pode otimizar as opções de CPU para se adequarem a workloads ou necessidades de negócios específicos. Para obter mais informações, consulte Criar um modelo de execução (p. 427) .	11 de julho de 2018
Marcação de Hosts dedicados	15/11/2016	Você pode marcar seus Hosts dedicados. Para obter mais informações, consulte Marcação de Hosts dedicados (p. 367) .	3 de julho de 2018
i3.metalInstâncias do	15/11/2016	As instâncias i3.metal fornecem às aplicações acesso direto aos recursos físicos do servidor host, como os processadores e a memória. Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 222) .	17 de maio de 2018
Obter a saída mais recente do console	15/11/2016	Você pode recuperar a saída mais recente do console para alguns tipos de instância usando o comando get-console-output da AWS CLI.	9 de maio de 2018
Otimizar as opções de CPU	15/11/2016	Ao executar uma instância, você pode otimizar as opções de CPU para atender a workloads ou necessidades de negócios específicas: Para obter mais informações, consulte Otimizar as opções de CPU (p. 582) .	8 de maio de 2018
EC2 Fleet	15/11/2016	Você pode usar a EC2 Fleet para executar um grupo de instâncias em tipos de instância do EC2 e zonas de disponibilidade diferentes, e entre modelos de compra sob demanda, instância reservada e instância spot. Para obter mais informações, consulte EC2 Fleet (p. 712) .	2 de maio de 2018
Instâncias sob demanda em Frotas spot	15/11/2016	Você pode incluir uma solicitação de capacidade sob demanda na solicitação de frota spot para garantir que você sempre tenha capacidade de instância. Para obter mais informações, consulte Frota spot (p. 761) .	2 de maio de 2018
Marcar snapshots do EBS na criação	15/11/2016	Você pode aplicar tags a snapshots durante a criação. Para obter mais informações, consulte Criar snapshots de Amazon EBS (p. 1298) .	2 de abril de 2018
Alterar placement groups	15/11/2016	Você pode mover uma instância para dentro ou para fora de um placement group, ou alterar o placement group da instância. Para obter mais informações, consulte Alterar o placement group de uma instância (p. 1054) .	1 de março de 2018
IDs mais longos de recursos	15/11/2016	Você pode habilitar o formato de ID mais longo para outros tipos de recursos. Para obter mais informações, consulte IDs de recursos (p. 1545) .	9 de fevereiro de 2018

Recurso	Versão da API	Descrição	Data de lançamento
Melhorias na performance da rede	15/11/2016	As instâncias de fora de um placement group de cluster podem agora se beneficiar de uma maior largura de banda para enviar ou receber tráfego de rede entre as outras instâncias ou o Amazon S3. Para obter mais informações, consulte Recursos de redes e armazenamento (p. 155) .	24 de janeiro de 2018
Marcar endereços IP elásticos	15/11/2016	Você pode marcar seus endereços IP elásticos. Para obter mais informações, consulte Aplicar uma tag em um endereço IP elástico (p. 996) .	21 de dezembro de 2017
Amazon Time Sync Service	15/11/2016	Você pode usar o Amazon Time Sync Service para manter a precisão da hora na instância. Para obter mais informações, consulte Definir o horário para uma instância do Windows. (p. 601) .	29 de novembro de 2017
T2 ilimitada	15/11/2016	As instâncias T2 ilimitadas podem apresentar uma intermitência acima da linha de base pelo tempo que for necessário. Para obter mais informações, consulte Instâncias expansíveis (p. 169) .	29 de novembro de 2017
Modelos de execução	15/11/2016	Um modelo de execução pode conter todos ou alguns parâmetros necessários à execução de uma instância, de modo que você não precise especificá-las todas as vezes que executar uma instância. Para obter mais informações, consulte Executar uma instância a partir de um modelo de execução (p. 425) .	29 de novembro de 2017
Posicionamento disseminado	15/11/2016	Os placement groups de distribuição são recomendados para aplicações com uma pequena quantidade de instâncias críticas que devem ser mantidas separadas umas das outras. Para obter mais informações, consulte Placement groups de distribuição (p. 1046) .	29 de novembro de 2017
Instâncias H1	15/11/2016	As instâncias H1 são projetadas para workloads de big data de alta performance. Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 222) .	28 de novembro de 2017
Instâncias M5	15/11/2016	As instâncias M5 são instâncias de computação de propósito geral. Elas permitem um equilíbrio entre os recursos de computação, memória, armazenamento e rede.	28 de novembro de 2017
Hibernação da instância spot	15/11/2016	O serviço spot pode hibernar instâncias spot em caso de interrupção. Para obter mais informações, consulte Hibernar Instâncias spot interrompida (p. 338) .	28 de novembro de 2017

Recurso	Versão da API	Descrição	Data de lançamento
Monitoramento do objetivo da frota spot	15/11/2016	Você pode configurar políticas de dimensionamento com monitoramento do objetivo para a frota spot. Para obter mais informações, consulte Alterar a escala da frota spot usando as políticas de monitoramento do objetivo (p. 794) .	17 de novembro de 2017
A frota spot integra-se ao Elastic Load Balancing	15/11/2016	Você pode associar um ou mais load balancers a uma frota spot.	10 de novembro de 2017
Instâncias X1e	15/11/2016	As instâncias X1e são ideais para bancos de dados de alta performance, bancos de dados de memória e outras aplicações empresariais que consomem muita memória. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 211) .	28 de novembro de 2017
Instâncias C5	15/11/2016	As instâncias C5 são desenvolvidas para aplicações de computação pesada. Para obter mais informações, consulte Instâncias otimizadas para computação (p. 204) .	6 de novembro de 2017
Mesclagem e divisão do Instâncias reservadas conversíveis	15/11/2016	Você pode trocar (mesclar) dois ou mais Instâncias reservadas conversíveis por um novo Instância reservada convertível. Você também pode usar o processo de modificação para dividir um Instância reservada convertível em reservas menores. Para obter mais informações, consulte Trocar Instâncias reservadas conversíveis (p. 293) .	6 de novembro de 2017
Instâncias P3	15/11/2016	As instâncias P3 são instâncias de GPU otimizadas para computação. Para obter mais informações, consulte Windows Instâncias computacionais aceleradas do (p. 228) .	25 de outubro de 2017
Modificar a locação da VPC	15/11/2016	Você pode alterar o atributo de locação da instância da VPC de <code>dedicated</code> para <code>default</code> . Para obter mais informações, consulte Alterar a locação de uma VPC (p. 390) .	16 de outubro de 2017
Parar em interrupção	15/11/2016	Você pode especificar se o Amazon EC2 deve parar ou encerrar as Instâncias spot quando elas são interrompidas. Para obter mais informações, consulte Comportamentos de interrupção (p. 337) .	18 de setembro de 2017
Marcar gateways NAT	15/11/2016	Você pode marcar o gateway NAT. Para obter mais informações, consulte Marcar com tag os recursos do (p. 1555) .	7 de setembro de 2017
Descrições de regras do security group	15/11/2016	Você pode adicionar descrições às regras do security group. Para obter mais informações, consulte Regras de grupos de segurança (p. 1218) .	31 de agosto de 2017

Recurso	Versão da API	Descrição	Data de lançamento
Elastic Graphics	15/11/2016	Anexe aceleradores de Elastic Graphics a suas instâncias para acelerar a performance de gráficos de suas aplicações. Para obter mais informações, consulte Amazon Elastic Graphics (p. 850) .	29 de agosto de 2017
Recuperar endereços IP elásticos	15/11/2016	Se você liberar um endereço IP elástico para usar em um VPC, poderá recuperá-lo. Para obter mais informações, consulte Recuperar um endereço IP elástico (p. 1000) .	11 de agosto de 2017
Marcar instâncias de frota spot	15/11/2016	Você pode configurar sua frota spot para marcar automaticamente as instâncias que ela executa.	24 de julho de 2017
Instâncias G3	15/11/2016	As instâncias G3 fornecem uma plataforma de alta performance, econômica, para aplicações gráficas que utilizam DirectX ou OpenGL. As instâncias G3 também fornecem recursos de NVIDIA GRID Virtual Workstation, oferecendo suporte a 4 monitores com resoluções de até 4096x2160. Para obter mais informações, consulte Windows Instâncias computacionais aceleradas (p. 228) .	13 de julho de 2017
Recursos de tags durante a criação	15/11/2016	Você pode aplicar tags a instâncias e volumes durante a criação. Para obter mais informações, consulte Marcar com tag os recursos do (p. 1555) . Além disso, você pode usar permissões em nível de recurso baseadas em tags para controlar as tags que são aplicadas. Para obter mais informações, consulte, Conceder permissão para marcar recursos durante a criação (p. 1145) .	28 de março de 2017
Instâncias I3	15/11/2016	As instâncias I3 são instâncias otimizadas para armazenamento. Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 222) .	23 de fevereiro de 2017
Executar modificações em volumes do EBS anexados	15/11/2016	Com a maioria dos volumes do EBS anexados à maioria das instâncias do EC2, você pode modificar o tamanho, o tipo e as IOPS do volume sem desanexar o volume ou parar a instância. Para obter mais informações, consulte Volumes elásticos do Amazon EBS (p. 1409) .	13 de fevereiro de 2017
Anexar uma função da IAM	15/11/2016	Você pode anexar, desanexar ou substituir uma função da IAM para uma instância existente. Para obter mais informações, consulte Funções do IAM para Amazon EC2 (p. 1195) .	9 de fevereiro de 2017
Instâncias spot dedicadas	15/11/2016	É possível executar Instâncias spot em hardware de único locatário em uma nuvem privada virtual (VPC). Para obter mais informações, consulte Especificar uma locação para suas Instâncias spot (p. 311) .	19 de janeiro de 2017

Recurso	Versão da API	Descrição	Data de lançamento
Suporte a IPv6	15/11/2016	Você pode associar um CIDR IPv6 às suas VPC e sub-redes e atribuir endereços IPv6 a instâncias em sua VPC. Para obter mais informações, consulte Endereçamento IP de instâncias do Amazon EC2 (p. 956) .	1º de dezembro de 2016
Instâncias R4	15/09/2016	As instâncias R4 são instâncias otimizadas para memória. As instâncias R4 são ideais para workloads com uso intensivo de memória e sensíveis à latência, como business intelligence (BI), análise e mineração de dados, bancos de dados na memória, cache de memória de escala Web distribuída e processamento em tempo real da performance de aplicações de Big Data não estruturado. Para obter mais informações, consulte Instâncias otimizadas para memória (p. 211)	30 de novembro de 2016
Novos tipos de instância t2.xlarge e t2.2xlarge	15/09/2016	As instâncias T2 são projetadas para fornecer performance base moderada e capacidade de intermitênciam para obter performance significativamente mais alta conforme necessário para sua workload. São destinadas para aplicações que precisam de capacidade de resposta, alta performance por períodos de tempo limitados e de baixo custo. Para obter mais informações, consulte Instâncias expansíveis (p. 169) .	30 de novembro de 2016
Instâncias P2	15/09/2016	As instâncias P2 usam GPUs NVIDIA Tesla K80 e são projetadas para computação de GPU de uso geral que usa os modelos de programação CUDA ou OpenCL. Para obter mais informações, consulte Windows Instâncias computacionais aceleradas (p. 228) .	29 de setembro de 2016
m4.16xlargeInstâncias	01/04/2016	Expande o intervalo da família M4 de finalidade geral com a introdução de instâncias m4.16xlarge, com 64 vCPUs e 256 GiB de RAM.	6 de setembro de 2016
Escalabilidade automática para frota spot		Agora você pode configurar políticas de escalabilidade para a frota spot. Para obter mais informações, consulte Escalabilidade automática para frota spot (p. 792) .	1º de setembro de 2016
Elastic Network Adapter (ENA)	01/04/2016	Agora você pode usar o ENA para rede avançada. Para obter mais informações, consulte Suporte a redes avançadas (p. 1029) .	28 de junho de 2016
Suporte avançado para visualização e modificação de IDs mais longos	01/04/2016	Agora você pode visualizar e modificar as configurações de IDs mais longos para outros usuários do IAM funções do IAM ou usuários root. Para obter mais informações, consulte IDs de recursos (p. 1545) .	23 de junho de 2016

Recurso	Versão da API	Descrição	Data de lançamento
Copiar snapshots do Amazon EBS criptografados entre contas da AWS	01/04/2016	Agora é possível copiar snapshots do EBS criptografados entre contas da AWS. Para obter mais informações, consulte Copiar um snapshot do Amazon EBS. (p. 1317) .	21 de junho de 2016
Capturar uma captura de tela do console de uma instância	01/10/2015	Agora é possível obter informações adicionais ao depurar instâncias não acessíveis. Para obter mais informações, consulte Solucionar problemas de uma instância não acessível (p. 1581) .	24 de maio de 2016
Instâncias X1	01/10/2015	Instâncias otimizadas para memória desenvolvidas para execução em bancos de dados na memória, mecanismos de processamento de big data e aplicações de computação de alta performance (HPC). Para obter mais informações, consulte Instâncias otimizadas para memória (p. 211) .	18 de maio de 2016
Dois novos tipos de volume do EBS	01/10/2015	Agora você pode criar HDD otimizado para taxa de transferência (st1) e volumes de disco rígido frio (sc1). Para obter mais informações, consulte Tipos de volume do Amazon EBS (p. 1247) .	19 de abril de 2016
Inclusão de novas métricas NetworkPacketsIn e NetworkPacketsOut para o Amazon EC2		Inclusão de novas métricas NetworkPacketsIn e NetworkPacketsOut para o Amazon EC2. Para obter mais informações, consulte Métricas de instância (p. 902) .	23 de março de 2016
Métricas do CloudWatch para frota spot		Agora você pode obter as métricas do CloudWatch para sua frota spot. Para obter mais informações, consulte Métricas do CloudWatch para frota spot (p. 790) .	21 de março de 2016
Instâncias programadas	01/10/2015	As instâncias reservadas programadas (instâncias programadas) permitem adquirir Reservas de Capacidade que se repetem diariamente, semanalmente ou mensalmente, com uma hora de início e duração especificadas. Para obter mais informações, consulte Scheduled Reserved Instances (p. 298) .	13 de janeiro de 2016
IDs mais longos de recursos	01/10/2015	Gradualmente, estamos introduzindo IDs de comprimento mais longo para alguns tipos de recursos do Amazon EC2 e do Amazon EBS. Durante o período de aceitação, você pode habilitar o formato mais longo de ID para tipos de recursos compatíveis. Para obter mais informações, consulte IDs de recursos (p. 1545) .	13 de janeiro de 2016

Recurso	Versão da API	Descrição	Data de lançamento
Supporte do DNS para o ClassicLink	01/10/2015	Você pode habilitar o suporte a DNS do ClassicLink para sua VPC de forma que os hostnames de DNS sejam endereçados entre instâncias vinculadas do EC2-Classic e instâncias na resolução da VPC para endereços IP privados e não para endereços IP públicos. Para obter mais informações, consulte Habilitar o suporte a DNS do ClassicLink (p. 1113) .	11 de janeiro de 2016
Novo tipo de instância <code>t2.nano</code>	01/10/2015	As instâncias T2 são projetadas para fornecer performance base moderada e capacidade de intermitência para obter performance significativamente mais alta conforme necessário para seu workload. São destinadas para aplicações que precisam de capacidade de resposta, alta performance por períodos de tempo limitados e de baixo custo. Para obter mais informações, consulte Instâncias expansíveis (p. 169) .	15 de dezembro de 2015
Hosts dedicados	01/10/2015	Um host de Amazon EC2 dedicado é um servidor físico com capacidade de instância dedicado para seu uso. Para obter mais informações, consulte Dedicated Hosts (p. 349) .	23 de novembro de 2015
Duração da instância spot	01/10/2015	Agora você pode especificar uma duração para Instâncias spot. Para obter mais informações, consulte Definir uma duração para suas Instâncias spot (p. 311) .	6 de outubro de 2015
Solicitação de modificação de frota spot	01/10/2015	Agora é possível modificar a capacidade de destino de sua solicitação de frota spot. Para obter mais informações, consulte Modificar uma solicitação de frota spot (p. 787) .	29 de setembro de 2015
Estratégia diversificada de alocação de frota spot	15/04/2015	Agora você pode alocar instâncias spot em vários grupos spot usando uma única solicitação de frota spot. Para obter mais informações, consulte Estratégia de alocação para Instâncias spot (p. 762) .	15 de setembro de 2015
Peso de instâncias de frotas spot	15/04/2015	Agora você pode definir as unidades de capacidade com que cada tipo de instância contribui para a performance de sua aplicação, e ajustar o valor a ser pago por Instâncias spot para cada grupo spot de forma correspondente. Para obter mais informações, consulte Peso de instâncias de frotas spot (p. 768) .	31 de agosto de 2015
Nova ação de alarme de reinicialização e nova função do IAM para uso com ações de alarme		Adicionada a ação de alarme de reinicialização e a nova função do IAM para uso com ações de alarme. Para obter mais informações, consulte Criar alarmes para interromper, encerrar, reiniciar ou recuperar uma instância (p. 924) .	23 de julho de 2015

Recurso	Versão da API	Descrição	Data de lançamento
Novo tipo de instância t2.large		As instâncias T2 são projetadas para fornecer performance base moderada e capacidade de intermitência para obter performance significativamente mais alta conforme necessário para seu workload. São destinadas para aplicações que precisam de capacidade de resposta, alta performance por períodos de tempo limitados e de baixo custo. Para obter mais informações, consulte Instâncias expansíveis (p. 169) .	16 de junho de 2015
Instâncias M4		A próxima geração de instâncias para finalidade geral que fornecem um equilíbrio de computação, memória e recursos de rede. As instâncias M4 são habilitadas por um processador Intel de 2,4 GHz Intel® Xeon® E5 2676v3 (Haswell) personalizado com AVX2.	11 de junho de 2015
Spot Fleets	15/04/2015	É possível gerenciar uma coleção ou uma frota de instâncias spot em vez de gerenciar solicitações separadas de instância spot. Para obter mais informações, consulte Frota spot (p. 761) .	18 de maio de 2015
Migrar endereços IP elásticos para o EC2-Classic	15/04/2015	É possível migrar um endereço IP elástico que foi alocado para uso em EC2-Classic para ser usado em uma VPC. Para obter mais informações, consulte Migrar um endereço IP elástico do EC2-Classic (p. 1104) .	15 de maio de 2015
Importar VMs com vários discos como AMIs	01/03/2015	O processo de VM Import agora oferece suporte à importação de VMs com vários discos como AMIs. Para obter mais informações, consulte Como importar uma VM como uma imagem usando o VM Import/Export no Guia do usuário de VM Import/Export.	23 de abril de 2015
Novo tipo de instância g2.8xlarge		A nova instância g2.8xlarge tem suporte de quatro GPUs NVIDIA de alta performance, tornando-a ideal para workloads de computação de GPU incluindo renderização em grande escala, transcodificação, Machine Learning e outras workloads de servidor que exigem potência massiva de processamento paralelo.	7 de abril de 2015

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias D2		<p>As instâncias com armazenamento denso que são otimizadas para aplicações que exigem acesso sequencial a uma grande quantidade de dados no armazenamento de instâncias anexado diretamente. As instâncias D2 são projetadas para oferecer melhor preço/performance na família de armazenamento denso. Habilitadas por processadores de 2,4 GHz Intel® Xeon® E5 2676v3 (Haswell), as instâncias D2 melhoram as instâncias HS1 fornecendo poder computacional adicional, mais memória e redes avançadas. Além disso, as instâncias D2 estão disponíveis em quatro tamanhos de instância com opções de armazenamento de 6, 12, 24 e 48 TB.</p> <p>Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 222).</p>	24 de março de 2015
Systems Manager		O Systems Manager permite configurar e gerenciar as instâncias do EC2.	17 de fevereiro de 2015
Systems Manager para Microsoft SCVMM 1.5		Agora você pode usar o Systems Manager para Microsoft SCVMM para executar uma instância e para importar uma VM do SCVMM para o Amazon EC2. Para obter mais informações, consulte Criar uma instância do EC2 (p. 1651) e Importar sua máquina virtual (p. 1656) .	21 de janeiro de 2015
Recuperação automática de instâncias do EC2		<p>Você pode criar um alarme do Amazon CloudWatch que monitore uma instância do Amazon EC2 e recupere-a automaticamente se ocorrer um problema devido a uma falha de hardware subjacente ou um problema que exija o envolvimento da AWS para repará-lo. Uma instância recuperada é idêntica à instância original incluindo o ID da instância, os endereços IP e todos os metadados da instância.</p> <p>Para obter mais informações, consulte Recuperar a instância (p. 480).</p>	12 de janeiro de 2015

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias C4		<p>A próxima geração de instâncias otimizadas para computação que fornecem performance muito alta da CPU a um preço econômico. As instâncias C4 são baseadas em processadores de 2,9 GHz Intel® Xeon® E5-2666 v3 (Haswell) personalizados. Com Turbo Boost adicional, a velocidade do clock do processador em instâncias C4 pode atingir até 3,5 GHz com 1 ou 2 núcleos turbo. Expandindo as capacidades das instâncias C3 otimizadas para computação, as instâncias C4 oferecem aos clientes a mais alta performance de processador entre as instâncias do EC2. Idealmente, essas instâncias são ideais para aplicativos web de alto tráfego, veiculação de anúncios, processamento em lote, codificação de vídeo, análises distribuídas, física de alta energia, análise de genoma e dinâmica de fluidos computacional.</p> <p>Para obter mais informações, consulte Instâncias otimizadas para computação (p. 204).</p>	11 de janeiro de 2015
ClassicLink	01/10/2014	<p>O ClassicLink permite vincular sua instância do EC2-Classic a uma VPC em sua conta. Você pode associar security groups da VPC à instância do EC2-Classic habilitando a comunicação entre sua instância do EC2-Classic e as instâncias em sua VPC usando endereços IP privados. Para obter mais informações, consulte ClassicLink (p. 1107).</p>	7 de janeiro de 2015
Notificações de encerramento de instância spot		<p>A melhor maneira de proteger-se contra a interrupção de instância spot é configurar a aplicação para ser tolerante a falhas. Além disso, você pode aproveitar os avisos de encerramento de instância spot, que enviam um aviso dois minutos antes de o Amazon EC2 encerrar a instância spot.</p> <p>Para obter mais informações, consulte Avisos de interrupção de instância spot (p. 341).</p>	5 de janeiro de 2015
Systems Manager para Microsoft SCVMM		<p>O Systems Manager para Microsoft SCVMM fornece uma interface simples e fácil de usar para gerenciamento de recursos da AWS, como instâncias do EC2, no Microsoft SCVMM. Para obter mais informações, consulte AWS Systems Manager para Microsoft System Center VMM (p. 1646).</p>	29 de outubro de 2014
DescribeVolumesSupport à paginação de	01/09/2014	<p>A API <code>DescribeVolumes</code> agora oferece suporte à paginação dos resultados com os parâmetros <code>MaxResults</code> e <code>NextToken</code>. Para obter mais informações, consulte DescribeVolumes no Amazon EC2 API Reference.</p>	23 de outubro de 2014

Recurso	Versão da API	Descrição	Data de lançamento
Adicionado o suporte para Amazon CloudWatch Logs		Você pode usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar o sistema, a aplicação e os arquivos de log personalizados em suas instâncias ou em outras origens. Em seguida, você pode recuperar os dados de log associados do CloudWatch Logs usando o console do Amazon CloudWatch, os comandos do CloudWatch Logs na AWS CLI ou o SDK do CloudWatch Logs.	10 de julho de 2014
Instâncias T2	15/06/2014	As instâncias T2 são projetadas para fornecer performance base moderada e capacidade de intermitência para obter performance significativamente mais alta conforme necessário para seu workload. São destinadas para aplicações que precisam de capacidade de resposta, alta performance por períodos de tempo limitados e de baixo custo. Para obter mais informações, consulte Instâncias expansíveis (p. 169) .	30 de junho de 2014
Nova página EC2 Service Limits		Use a página EC2 Service Limits no console do Amazon EC2 para visualizar os limites atuais dos recursos fornecidos pelo Amazon EC2 e a Amazon VPC por região.	19 de junho de 2014
Volumes de Amazon EBS Finalidade geral (SSD)	01/05/2014	Os volumes Finalidade geral (SSD) oferecem armazenamento econômico ideal para uma ampla variedade de workloads. Esses volumes proporcionam latências de milissegundos de um dígito, capacidade de intermitência de 3.000 IOPS por períodos estendidos e uma performance básica de 3 IOPS/GiB. Os volumes SSD de uso geral podem variar de tamanho entre 1 GiB e 1 TiB. Para obter mais informações, consulte Volumes de Finalidade geral (SSD) (gp2) (p. 1251) .	16 de junho de 2014
Windows Server 2012 R2		As AMIs para Windows Server 2012 R2 usam os novos drivers PV da AWS. Para obter mais informações, consulte AWS Drivers PV (p. 561) .	3 de junho de 2014
AWS Management Pack		AWSO Management Pack agora oferece suporte para o System Center Operations Manager 2012 R2. Para obter mais informações, consulte AWS Management Pack for Microsoft System Center (p. 1661) .	22 de maio de 2014

Recurso	Versão da API	Descrição	Data de lançamento
Amazon EBS encryption	01/05/2014	O Criptografia de Amazon EBS oferece criptografia sem interrupção dos volumes de dados do EBS, bem como de snapshots, eliminando a necessidade de criar e manter uma infraestrutura de gerenciamento de chaves de segurança. A criptografia do EBS ativa a segurança dos dados em repouso, criptografando os dados usando as Chaves gerenciadas pela AWS . A criptografia ocorre nos servidores que hospedam as instâncias do EC2, oferecendo criptografia de dados durante seu trânsito entre as instâncias do EC2 e armazenamento do EBS. Para obter mais informações, consulte Criptografia de Amazon EBS (p. 1422) .	21 de maio de 2014
Instâncias R3	01/02/2014	Instâncias otimizadas para memória com a melhor faixa de preços por GiB de RAM e de alta performance. Idealmente, essas instâncias são ideais para bancos de dados relacionais e NoSQL, soluções de análise na memória, computação científica e outras aplicações com consumo intensivo de memória que podem se beneficiar de mais memória vCPU, alta performance de computação e dos recursos de rede avançada das instâncias R3. Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte Amazon EC2 Instance Types (Tipos de instância do Amazon EC2).	9 de abril de 2014
Relatórios de uso do Amazon EC2		Os relatórios de uso do Amazon EC2 são um conjunto de relatórios que mostram os custos e os dados de uso do EC2. Para obter mais informações, consulte Relatórios de uso do Amazon EC2 (p. 1569) .	28 de janeiro de 2014
Instâncias M3 adicionais	15/10/2013	Os tamanhos de instâncias M3 m3.medium e m3.large agora são compatíveis. Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte Amazon EC2 Instance Types (Tipos de instância do Amazon EC2).	20 de janeiro de 2014
Instâncias I2	15/10/2013	Essas instâncias fornecem IOPS muito altos. As instâncias I2 também oferecem suporte à rede avançada que oferece latências aprimoradas entre instâncias, menor oscilação de rede e performance de pacotes por segundo (PPS) significativamente mais alta. Para obter mais informações, consulte Instâncias otimizadas para armazenamento (p. 222) .	19 de dezembro de 2013

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias M3 atualizadas	15/10/2013	Os tamanhos de instâncias M3, m3.xlarge e m3.2xlarge, agora oferecem suporte ao armazenamento de instâncias com volumes SSD.	19 de dezembro de 2013
Permissões em nível de recurso para RunInstances	15/10/2013	Agora você pode criar políticas no AWS Identity and Access Management para controlar permissões em nível de recurso para a ação da API RunInstances do Amazon EC2. Para obter mais informações e políticas de exemplo, consulte Identity and Access Management para o Amazon EC2 (p. 1137) .	20 de novembro de 2013
Instâncias C3	15/10/2013	Instâncias otimizadas para computação que fornecem performance muito alta de CPU a um preço econômico. As instâncias C3 também oferecem suporte à rede avançada que oferece latências aprimoradas entre instâncias, menor oscilação de rede e performance de pacotes por segundo (PPS) significativamente mais alta. Idealmente, essas instâncias são ideais para aplicativos web de alto tráfego, veiculação de anúncios, processamento em lote, codificação de vídeo, análises distribuídas, física de alta energia, análise de genoma e dinâmica de fluidos computacional. Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte Amazon EC2 Instance Types (Tipos de instância do Amazon EC2).	14 de novembro de 2013
Execução de uma instância no AWS Marketplace		Agora você pode executar uma instância no AWS Marketplace usando o Launch Wizard do Amazon EC2. Para obter mais informações, consulte Executar uma instância AWS Marketplace (p. 441) .	11 de novembro de 2013
Instâncias G2	01/10/2013	Idealmente, essas instâncias são ideais para serviços de criação de vídeo, visualizações 3D, transmissão de aplicações com consumo intensivo de gráficos e outras workloads do servidor que exigem potência de processamento paralelo massivo. Para obter mais informações, consulte Windows Instâncias computacionais aceleradas (p. 228) .	4 de novembro de 2013
Novo assistente de execução		Há um novo assistente de execução reprojetado do EC2. Para obter mais informações, consulte É possível executar uma instância usando o assistente de execução de instância. (p. 419) .	10 de outubro de 2013
Modificação de instâncias reservadas do Amazon EC2	15/08/2013	Agora você pode modificar instâncias reservadas em uma região.	11 de setembro de 2013

Recurso	Versão da API	Descrição	Data de lançamento
Atribuição de um endereço IP público	15/07/2013	Agora você pode atribuir um endereço IP público ao executar uma instância em uma VPC. Para obter mais informações, consulte Atribuir um endereço IPv4 público durante a execução da instância (p. 961) .	20 de agosto de 2013
Concessão de permissões em nível de recurso	15/06/2013	O Amazon EC2 oferece suporte aos novos Nomes de recurso da Amazon (ARNs) e a chaves de condição. Para obter mais informações, consulte Políticas do IAM no Amazon EC2 (p. 1139) .	8 de julho de 2013
Cópias incrementais de snapshot	01/02/2013	Agora você pode executar cópias incrementais de snapshot. Para obter mais informações, consulte Copiar um snapshot do Amazon EBS. (p. 1317) .	11 de junho de 2013
AWS Management Pack		O AWS Management Pack vincula as instâncias do Amazon EC2 e os sistemas operacionais Windows ou Linux que são executados nelas. O AWS Management Pack é uma extensão do Microsoft System Center Operations Manager. Para obter mais informações, consulte AWS Management Pack for Microsoft System Center (p. 1661) .	8 de maio de 2013
Nova página Tags		Há uma nova página Tags no console do Amazon EC2. Para obter mais informações, consulte Marcar com tag os recursos do Amazon EC2 (p. 1554) .	04 de abril de 2013
Tipos de instâncias otimizadas para EBS adicionais	01/02/2013	Os seguintes tipos de instância agora podem ser executados como instâncias otimizadas para EBS: <code>c1.xlarge</code> , <code>m2.2xlarge</code> , <code>m3.xlarge</code> e <code>m3.2xlarge</code> . Para obter mais informações, consulte Instâncias otimizadas para Amazon EBS (p. 1440) .	19 de março de 2013
Drivers de PV		Para saber como atualizar os drivers paravirtualizados (PV) na AMI do Windows, consulte Atualizar drivers de PV em instâncias do Windows (p. 565) .	Março de 2013
Cópia de uma AMI de uma região para outra	01/02/2013	Você pode copiar uma AMI de uma região para outra, o que permite executar instâncias consistentes em mais de uma região da AWS de maneira rápida e fácil. Para obter mais informações, consulte Copiar um AMI (p. 120) .	11 de março de 2013

Recurso	Versão da API	Descrição	Data de lançamento
Execução de instâncias em uma VPC padrão	01/02/2013	Sua conta da AWS é capaz de executar instâncias no EC2-Classic ou uma VPC ou somente em uma VPC, dependendo da região. Se você puder executar instâncias somente em uma VPC, criamos uma VPC padrão para você. Quando você executa uma instância, nós a executamos em sua VPC padrão, a menos que você crie uma VPC não padrão e a especifique ao executar a instância.	11 de março de 2013
Tipo de instância em cluster (cr1.8xlarge) com mais memória	01/12/2012	Ter grandes quantidades de memória acopladas à alta performance da CPU e da rede. Essas instâncias são ideais para análise na memória, análise de gráficos e aplicações de computação científica.	21 de janeiro de 2013
Tipo de instância de alto armazenamento (hs1.8xlarge)	01/12/2012	As instâncias de alto armazenamento fornecem uma alta densidade de armazenamento e alta performance de leitura e gravação sequencial por instância. São ideais para data warehousing, Hadoop/MapReduce e sistemas de arquivos paralelos.	20 de dezembro de 2012
Cópia de snapshot do EBS	01/12/2012	Você pode usar cópias de snapshots para criar backups de dados, para criar novos volumes do Amazon EBS ou para criar Imagens de máquina da Amazon (AMIs). Para obter mais informações, consulte Copiar um snapshot do Amazon EBS. (p. 1317) .	17 de dezembro de 2012
Verificações de métricas e status do EBS atualizadas para volumes do Provisioned IOPS SSD	01/10/2012	Atualizadas as métricas do EBS para incluir duas novas métricas para volumes do Provisioned IOPS SSD. Para obter mais informações, consulte Métricas do Amazon CloudWatch para o Amazon EBS (p. 1472) . Novas verificações de status também adicionadas para volumes do Provisioned IOPS SSD. Para obter mais informações, consulte Verificações de status do volume do EBS (p. 1282) .	20 de novembro de 2012

Recurso	Versão da API	Descrição	Data de lançamento
Suporte para o Windows Server 2012		<p>O Amazon EC2 agora fornece várias AMIs pré-configuradas do Windows Server 2012. Essas AMIs estão disponíveis imediatamente para uso em cada região e por cada tipo de instância de 64 bits. As AMIs oferecem suporte aos seguintes idiomas:</p> <ul style="list-style-type: none"> • Inglês • Chinês simplificado • Chinês tradicional • Chinês tradicional de Hong Kong • Japonês • Coreano • Português • Português (Brasil) • Tcheco • Holandês • Francês • Alemão • Húngaro • Italiano • Polonês • Russo • Espanhol • Sueco • Turco 	19 de novembro de 2012
Instâncias M3	01/10/2012	Há novos tipos de instâncias M3 extragrande e M3 dupla extragrande. Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte Amazon EC2 Instance Types (Tipos de instância do Amazon EC2).	31 de outubro de 2012
Status da solicitação de instância spot	01/10/2012	O status da solicitação da instância spot facilita a determinação do estado de suas solicitações spot.	14 de outubro de 2012
Marketplace de instâncias reservadas do Amazon EC2	15/08/2012	O Marketplace de instâncias reservadas correlaciona vendedores que têm instâncias reservadas do Amazon EC2 que não são mais necessárias a compradores que desejam adquirir capacidade adicional. As instâncias reservadas adquiridas e vendidas por meio do Marketplace de instâncias reservadas funcionam como qualquer outra instância reservada, com a exceção de que têm um período de vigência padrão menor que o período de vigência padrão total e podem ser vendidas a preços diferentes.	11 de setembro de 2012

Recurso	Versão da API	Descrição	Data de lançamento
Provisioned IOPS SSD para Amazon EBS	20/07/2012	Os volumes do Provisioned IOPS SSD fornecem alta performance previsível para workloads com uso intensivo de E/S, como aplicações de banco de dados que dependem de tempos de resposta consistentes e rápidos. Para obter mais informações, consulte Tipos de volume do Amazon EBS (p. 1247) .	31 de julho de 2012
Instâncias de E/S alta para o Amazon EC2	15/06/2012	As instâncias de E/S alta fornecem performance muito alta de E/S de disco, baixa latência usando armazenamento de instâncias local com base em SSD.	18 de julho de 2012
As funções do IAM em instâncias do Amazon EC2	01/06/2012	As funções do IAM para o Amazon EC2 fornecem: <ul style="list-style-type: none"> Chaves de acesso da AWS para aplicações que executam em instâncias do Amazon EC2. Rotação automática das chaves de acesso da AWS na instância do Amazon EC2. Permissões granulares para aplicações que executam em instâncias do Amazon EC2 que fazem solicitações para seus serviços da AWS. 	11 de junho de 2012
Os recursos de instâncias spot que facilitam a familiarização e o manuseio de possíveis interrupções.		Agora é possível gerenciar suas Instâncias spot da seguinte forma: <ul style="list-style-type: none"> Especifique o valor que você está disposto a pagar por Instâncias spot usando as configurações de execução de Auto Scaling e configure um cronograma para especificar o valor que você está disposto a pagar por Instâncias spot. Para obter mais informações, consulte Como executar Instâncias spot no grupo do Auto Scaling no Guia do usuário do Amazon EC2 Auto Scaling. Obter notificações quando as instâncias forem executadas ou encerradas. Usar modelos do AWS CloudFormation para executar instâncias spot em uma pilha com recursos da AWS. 	7 de junho de 2012
Exportação de instâncias do EC2 e time stamps para verificações de status para o Amazon EC2	01/05/2012	Suporte adicionado para exportar instâncias do Windows Server que você importou originalmente para o EC2. Suporte adicionado para time stamps no status da instância e no status do sistema para indicar a data e a hora em que uma verificação de status falhou.	25 de maio de 2012

Recurso	Versão da API	Descrição	Data de lançamento
Exportação de instâncias do EC2 e time stamps em verificações do status de instâncias e do sistema para a Amazon VPC	01/05/2012	Supporte adicionado para a exportação de instâncias do EC2 ao Citrix Xen, ao Microsoft Hyper-V e ao VMware vSphere. Supporte adicionado para time stamps em verificações de status de instâncias e do sistema.	25 de maio de 2012
Instância óctupla extragrande de computação em cluster	01/04/2012	Supporte adicionado para instâncias cc2.8xlarge em uma VPC.	26 de abril de 2012
AWS Marketplace AMIs	01/04/2012	Supporte adicionado para AMIs do AWS Marketplace .	19 de abril de 2012
Instâncias médias, suporte para 64 bits em todas as AMIs	15/12/2011	Supporte adicionado para um novo tipo de instância e informações 64 bits.	7 de março de 2012
Níveis de definição de preço de instâncias reservadas	15/12/2011	Adicionada uma nova seção que discute como beneficiar-se da definição de preço com desconto que está embutido nos níveis de definição de preço de instâncias reservadas.	5 de março de 2012
Interfaces de rede elástica (ENIs) para instâncias do EC2 na Amazon Virtual Private Cloud	01/12/2011	Adicionada nova seção sobre interfaces de rede elástica (ENIs) para instâncias do EC2 em uma VPC. Para obter mais informações, consulte Interfaces de rede elástica (p. 1002) .	21 de dezembro de 2011
Novos tipos de ofertas para instâncias reservadas do Amazon EC2	01/11/2011	Você pode escolher entre várias ofertas de instâncias reservadas que atendem a seu uso projetado da instância.	01 de dezembro de 2011
Status das instâncias do Amazon EC2	01/11/2011	Você pode visualizar detalhes adicionais sobre o status de suas instâncias, incluindo eventos programados planejados pela AWS que podem ter um impacto em suas instâncias. Essas atividades operacionais incluem reinicializações de instâncias necessárias para aplicar atualizações de software ou patches de segurança, ou a baixa de instâncias necessária quando há um problema de hardware. Para obter mais informações, consulte Monitorar o status das instâncias (p. 867) .	16 de novembro de 2011
Tipo de instância de computação em cluster do Amazon EC2		Adicionado suporte para a computação em cluster óctupla extragrande (cc2.8xlarge) para o Amazon EC2.	14 de novembro de 2011

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias spot na Amazon VPC	15/07/2011	Adição de informações sobre o suporte para Instâncias spot na Amazon VPC. Com essa atualização, os usuários podem executar Instâncias spot em uma nuvem privada virtual (VPC). Ao executar Instâncias spot em uma VPC, os usuários de Instâncias spot podem aproveitar os benefícios da Amazon VPC.	11 de outubro de 2011
Processo de VM Import simplificado para usuários das ferramentas da CLI	15/07/2011	O processo de VM Import está simplificado com a funcionalidade avançada do <code>ImportInstance</code> e do <code>ImportVolume</code> , que agora executarão o upload das imagens no Amazon EC2 depois de criar a tarefa de importação. Além disso, com a introdução do <code>ResumeImport</code> , os usuários poderão reiniciar um upload incompleto no ponto em que a tarefa parou.	15 de setembro de 2011
Suporte para importação do formato de arquivo VHD		O VM Import agora pode importar arquivos de imagem de máquina virtual em formato VHD. O formato de arquivo VHD é compatível com as plataformas de virtualização Citrix Xen e Microsoft Hyper-V. Com essa versão, o VM Import agora oferece suporte aos formatos de imagem RAW, VHD e VMDK (compatível com o VMware ESX). Para obter mais informações, consulte o VM Import/Export User Guide (Manual do usuário para importação/exportação de VMs) .	24 de agosto de 2011
Suporte para o Windows Server 2003 R2		O VM Import agora oferece suporte ao Windows Server 2003 (R2). Com essa versão, o VM Import oferece suporte a todas as versões do Windows Server que têm suporte do Amazon EC2.	24 de agosto de 2011
Atualização do Amazon EC2 VM Import Connector para VMware vCenter		Adicionadas informações sobre a versão 1.1 do Amazon EC2 VM Import Connector para o dispositivo virtual VMware vCenter (conector). Essa atualização inclui suporte de proxy para acesso à Internet, melhor manipulação de erros, barra de progresso de tarefas aprimorada e várias correções de erros.	27 de junho de 2011
Alterações na definição de preço de zonas de disponibilidade de Instâncias spot	15/05/2011	Adição de informações sobre o recurso de definição de preço de zonas de disponibilidade de Instâncias spot. Nessa versão, adicionamos novas opções de definição de preço de zonas de disponibilidade como parte das informações retornadas ao consultar as solicitações de instância spot e o histórico de preços spot. Essas adições facilitam a determinação do preço requerido para executar uma instância spot em uma zona de disponibilidade específica.	26 de maio de 2011

Recurso	Versão da API	Descrição	Data de lançamento
AWS Identity and Access Management		Adicionadas informações sobre o AWS Identity and Access Management (IAM), que permite que os usuários especifiquem quais ações do Amazon EC2 um usuário pode usar com recursos do Amazon EC2 em geral. Para obter mais informações, consulte Identity and Access Management para o Amazon EC2 (p. 1137) .	26 de abril de 2011
Instâncias dedicadas		Executadas em sua Amazon Virtual Private Cloud (Amazon VPC), as instâncias dedicadas são instâncias isoladas fisicamente no nível do hardware de host. As instâncias dedicadas permitem tirar proveito da Amazon VPC e da Nuvem AWS, com benefícios que incluem provisionamento elástico sob demanda e pagamento apenas pelo que você usa e, ao mesmo tempo, isolando suas instâncias de computação do Amazon EC2 no nível do hardware. Para obter mais informações, consulte Dedicated Instances (p. 383) .	27 de março de 2011
Atualizações nas instâncias reservadas para o Console de Gerenciamento da AWS		As atualizações no Console de Gerenciamento da AWS facilitam que os usuários visualizem suas instâncias reservadas e comprem instâncias reservadas adicionais, incluindo instâncias reservadas dedicadas.	27 de março de 2011
Suporte para o Windows Server 2008 R2		O Amazon EC2 agora fornece várias AMIs pré-configuradas do Windows Server 2008 R2. Essas AMIs estão disponíveis imediatamente para uso em cada região e na maioria dos tipos de instância de 64 bits excluindo as famílias de t1.micro e de HPC. As AMIs oferecerão suporte aos seguintes idiomas.	15 de março de 2011
Informações de metadados	01/01/2011	Adicionadas informações sobre os metadados para refletir as alterações na versão 2011-01-01. Para obter mais informações, consulte Metadados da instância e dados do usuário (p. 622) e Categorias de metadados da instância (p. 640) .	11 de março de 2011
Amazon EC2 VM Import Connector para VMware vCenter		Adicionadas informações sobre o Amazon EC2 VM Import Connector para o dispositivo virtual VMware vCenter (conector). O conector é um plug-in para VMware vCenter que está integrado a VMware vSphere Client e fornece uma interface gráfica de usuário que pode ser usada para importar as máquinas virtuais do VMware para o Amazon EC2.	3 de março de 2011
Forçar desanexação de volume		Agora você pode usar o AWS Management Console para forçar o desapego de um volume do Amazon EBS de uma instância. Para obter mais informações, consulte Desanexar um volume do Amazon EBS de uma instância Windows (p. 1290) .	23 de fevereiro de 2011

Recurso	Versão da API	Descrição	Data de lançamento
Proteção contra encerramento de instância		Agora você pode usar o Console de Gerenciamento da AWS para impedir que uma instância seja encerrada. Para obter mais informações, consulte Habilitar a proteção contra encerramento (p. 476) .	23 de fevereiro de 2011
VM Import	15/11/2010	Adicionadas informações sobre o VM Import que permite importar uma máquina virtual ou um volume no Amazon EC2. Para obter mais informações, consulte o VM Import/Export User Guide (Manual do usuário para importação/exportação de VMs) .	15 de dezembro de 2010
Monitoramento básico para instâncias	31/08/2010	Adicionadas informações sobre o monitoramento básico de instâncias do EC2.	12 de dezembro de 2010
Filtros e tags	31/08/2010	Adicionadas informações sobre recursos de listagem, filtragem e marcação. Para obter mais informações, consulte Listar e filtrar seus recursos (p. 1546) e Marcar com tag os recursos do Amazon EC2 (p. 1554) .	19 de setembro de 2010
Execução de instância idempotente	31/08/2010	Adicionadas informações sobre garantia de idempotência ao executar instâncias.	19 de setembro de 2010
Microinstâncias	15/06/2010	O Amazon EC2 oferece o tipo de instância <code>t1.micro</code> para certos tipos de aplicações. Para obter mais informações, consulte Instâncias expansíveis (p. 169) .	8 de setembro de 2010
AWS Identity and Access Management para o Amazon EC2		O Amazon EC2 agora se integra ao AWS Identity and Access Management (IAM). Para obter mais informações, consulte Identity and Access Management para o Amazon EC2 (p. 1137) .	2 de setembro de 2010
Instâncias em cluster	15/06/2010	O Amazon EC2 oferece instâncias de computação em cluster para aplicações de computação de alta performance (HPC). Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte Amazon EC2 Instance Types (Tipos de instância do Amazon EC2) .	12 de julho de 2010
Designação de endereço IP da Amazon VPC	15/06/2010	Os usuários do Amazon VPC agora podem especificar o endereço IP para atribuir uma instância executada em uma VPC.	12 de julho de 2010
Monitoramento de Amazon CloudWatch para volumes de Amazon EBS		Monitoramento de Amazon CloudWatch agora está disponível automaticamente para volumes de Amazon EBS. Para obter mais informações, consulte Métricas do Amazon CloudWatch para o Amazon EBS (p. 1472) .	14 de junho de 2010

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias extragrandes com mais memória	30/11/2009	O Amazon EC2 agora oferece suporte a um tipo de instância extragrande com mais memória (m2.xlarge). Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte Amazon EC2 Instance Types (Tipos de instância do Amazon EC2).	22 de fevereiro de 2010
Instâncias reservadas com Windows		O Amazon EC2 agora oferece suporte a instâncias reservadas com o Windows.	22 de fevereiro de 2010