

---

# Amazon Elastic Compute Cloud

## Manual do usuário para instâncias do Linux



## Amazon Elastic Compute Cloud: Manual do usuário para instâncias do Linux

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 desprestigie 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	1
Serviços relacionados	2
Acessar o Amazon EC2	3
Definição de preço do Amazon EC2	4
Conformidade do PCI DSS	4
Configurar	5
Cadastrar-se no AWS	5
Criar um par de chaves	5
Crie um grupo de segurança	6
Tutorial de conceitos básicos	9
Overview	9
Prerequisites	10
Etapa 1: executar uma instância	10
Etapa 2: conectar-se à instância	11
Etapa 3: limpar a instância	11
Próximas etapas	12
Práticas recomendadas	13
Tutoriais	15
Instalar o LAMP no Amazon Linux 2	15
Etapa 1: Preparar o servidor LAMP	16
Etapa 2: Testar o servidor LAMP	19
Etapa 3: Proteger o servidor do banco de dados	20
Etapa 4: (opcional) instalar o phpMyAdmin	21
Troubleshoot	24
Tópicos relacionados	24
Configurar o SSL/TLS em Amazon Linux 2	25
Prerequisites	26
Etapa 1: habilitar o TLS no servidor	26
Etapa 2: obter um certificado assinado por uma CA	28
Etapa 3: testar e intensificar a configuração de segurança	33
Troubleshoot	36
Automação de certificados: Let's Encrypt com o Certbot no Amazon Linux 2	36
Hospedar um blog do WordPress no Amazon Linux 2	40
Prerequisites	41
Instalar o WordPress	41
Próximas etapas	48
Ajuda! Meu nome DNS público mudou e agora meu blog não está funcionando	49
Instalar o LAMP no Amazon Linux AMI	50
Etapa 1: Preparar o servidor LAMP	50
Etapa 2: Testar o servidor LAMP	54
Etapa 3: Proteger o servidor do banco de dados	55
Etapa 4: (opcional) instalar o phpMyAdmin	56
Troubleshoot	59
Tópicos relacionados	60
Configurar o SSL/TLS com a AMI do Amazon Linux	60
Prerequisites	61
Etapa 1: habilitar o TLS no servidor	61
Etapa 2: obter um certificado assinado por uma CA	63
Etapa 3: testar e intensificar a configuração de segurança	68
Troubleshoot	70
Imagens de máquina da Amazon	72
Usar uma AMI	72

Criar sua própria AMI .....	73
Comprar, compartilhar e vender AMIs .....	73
Cancelar o registro da AMI .....	74
Amazon Linux 2 e Amazon Linux AMI .....	74
Tipos de AMI .....	74
Permissões de execução .....	74
Armazenamento para o dispositivo raiz .....	75
Tipos de virtualização .....	77
Modos de inicialização .....	79
Considerations .....	80
Requisitos para executar uma instância com UEFI .....	80
Determinar o parâmetro de modo de inicialização de uma AMI .....	81
Determinar os modos de inicialização suportados por um tipo de instância .....	82
Determinar o modo de inicialização de uma instância .....	82
Determinar o modo de inicialização do sistema operacional .....	83
Definir o modo de inicialização de uma AMI .....	84
Localizar uma AMI do Linux .....	87
Localizar uma AMI do Linux usando o console do Amazon EC2 .....	87
Localizar uma AMI usando o AWS CLI .....	88
Localizar a AMI do Amazon Linux mais recente usando o Systems Manager .....	88
Use um parâmetro de Systems Manager para localizar uma AMI .....	89
AMIs compartilhadas .....	92
Encontrar AMIs compartilhadas .....	92
Tornar um AMI pública .....	95
Compartilhar uma AMI com contas específicas da AWS .....	96
Usar marcadores .....	97
Diretrizes para AMIs em Linux compartilhadas .....	98
AMIs pagas .....	102
Vender sua AMI .....	103
Localizar uma AMI paga .....	103
Comprar uma AMI paga .....	104
Obter o código do produto para sua instância .....	105
Usar suporte pago .....	105
Faturas para AMI pagas e compatíveis .....	106
Gerenciar suas assinaturas do AWS Marketplace .....	106
Ciclo de vida da AMI .....	106
Criar uma AMI .....	107
Copiar um AMI .....	144
Armazenar e restaurar uma AMI .....	149
Defasar uma AMI .....	155
Cancelar AMI do Linux .....	159
Automatizar o ciclo de vida da AMI com suporte do EBS .....	163
Usar criptografia com AMIs com EBS .....	163
Cenários de execução de instância .....	163
Cenários de cópia de imagem .....	166
Noções básicas sobre o faturamento da AMI .....	168
Campos de faturamento da AMI .....	169
Localizar informações de faturamento de AMI .....	170
Verificar cobranças da AMI em sua fatura .....	172
Amazon Linux .....	172
Disponibilidade do Amazon Linux .....	173
Conectar-se a uma instância do Amazon Linux .....	173
Identificar imagens do Amazon Linux .....	173
AWSFerramentas da linha de comando da .....	174
Repositório de pacotes .....	175
Biblioteca de extras (Amazon Linux 2) .....	178
Acessar pacotes de origem para referência .....	178

cloud-init .....	179
Assinar notificações do Amazon Linux .....	180
Executar Amazon Linux 2 no local .....	182
Kernel Live Patching .....	186
Kernels fornecidos pelo usuário .....	191
AMIs HVM (GRUB) .....	191
AMIs paravirtuais (PV-GRUB) .....	192
Configure a conexão de desktop MATE .....	197
Prerequisite .....	197
Configure a conexão RDP .....	197
Instâncias .....	200
Instâncias e AMIs .....	200
Instances .....	201
AMIs .....	203
Tipos de instância .....	203
Tipos de instâncias disponíveis .....	204
Especificações de hardware .....	208
Tipos de virtualização de AMI .....	209
Instâncias criadas no Sistema Nitro .....	210
Recursos de redes e armazenamento .....	211
Limites de instâncias .....	214
Propósito geral .....	214
Otimizadas para computação .....	273
Otimizado para memória .....	282
Otimizada para armazenamento .....	297
Computação acelerada .....	305
Localizar um tipo de instância do .....	326
Alterar o tipo de instância .....	327
Obter recomendações .....	334
Opções de compra de instância .....	338
Determinar o ciclo de vida da instância .....	338
On-Demand Instances .....	340
Reserved Instances .....	343
Instâncias programadas .....	387
Spot Instances .....	389
Dedicated Hosts .....	440
Dedicated Instances .....	475
On-Demand Capacity Reservations .....	481
Ciclo de vida da instância .....	503
Execução da instância .....	505
Interrupção e início de instância (somente instâncias baseadas no Amazon EBS) .....	505
Hibernação de instância (somente instâncias baseadas no Amazon EBS) .....	506
Reinicialização da instância .....	506
Desativação da instância .....	507
Encerramento de instância .....	507
Diferenças entre reinicialização, interrupção, hibernação e encerramento .....	507
Executar .....	509
Conecte-se .....	535
Interromper e iniciar .....	562
Hibernar .....	566
Reinicializar .....	583
Retirada .....	584
Encerrar .....	587
Recuperar .....	593
Configurar instâncias .....	595
Cenários de configuração comuns .....	595
Gerenciar software .....	596

Gerenciar usuários .....	602
Controle do estado do processador .....	604
Definir o horário .....	610
Otimizar as opções de CPU .....	616
Alterar o nome do host .....	637
Configurar um DNS dinâmico .....	640
Executar comandos na inicialização .....	642
Metadados da instância e dados do usuário .....	649
Elastic Inference .....	698
Identificar instâncias do .....	698
Inspecione o documento de identidade da instância .....	698
Inspecione o UUID do sistema .....	698
Frotas .....	700
EC2 Fleet .....	700
Limitações da Frota do EC2 .....	701
Instâncias expansíveis .....	701
Tipos de solicitação da Frota do EC2 .....	702
Estratégias de configuração da Frota do EC2 .....	720
Trabalhar com Frotas do EC2 .....	729
Frota spot .....	749
Tipos de solicitação da frota spot .....	749
Estratégias de configuração de frota spot .....	749
Trabalhar com frotas spot .....	757
Métricas do CloudWatch para frota spot .....	778
Escalabilidade automática para frota spot .....	780
Monitorar eventos da frota .....	787
Tipos de evento de Frota do EC2 .....	787
Tipos de evento de frota spot .....	791
Criar uma regra de EventBridge .....	796
Tutoriais .....	801
Tutorial: Usar a Frota do EC2 com ponderação de instâncias .....	802
Tutorial: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal .....	804
Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas .....	805
Tutorial: Usar frota spot com ponderação de instâncias .....	810
Exemplos de configuração .....	812
Exemplos de configuração de Frota do EC2 .....	812
Exemplos de configuração de frota spot .....	825
Quotas da frota .....	836
Monitor .....	838
Monitoramento automático e manual .....	839
Ferramentas de monitoramento automatizadas .....	839
Ferramentas de monitoramento manual .....	840
Melhores práticas de monitoramento .....	841
Monitorar o status das instâncias .....	841
Verificações de status de instâncias .....	841
Eventos agendados .....	848
Monitorar instâncias usando o CloudWatch .....	872
Habilitar o monitoramento detalhado .....	873
Listar métricas disponíveis .....	875
Obter estatísticas para métricas .....	888
Representar métricas em gráficos .....	896
Criar um alarme .....	896
Criar alarmes para interromper, encerrar, reinicializar ou recuperar uma instância .....	898
Automatizar o Amazon EC2 com o EventBridge .....	910
Monitorar métricas de memória e de disco .....	911
Coletar métricas usando o agente do CloudWatch .....	911
Obsoleto: coletar métricas usando os scripts de monitoramento do CloudWatch .....	911

Registrar em log as chamadas de APIs com o AWS CloudTrail .....	919
Informações sobre o Amazon EC2 e o Amazon EBS no CloudTrail .....	919
Noções básicas sobre entradas dos arquivos de log no Amazon EC2 e no Amazon EBS. ....	920
Auditar usuários que se conectam por EC2 Instance Connect .....	921
Redes .....	923
Regiões e zonas .....	923
Regions .....	924
Zonas de disponibilidade .....	928
Local Zones .....	930
Zonas do Wavelength .....	934
AWS Outposts .....	936
Endereçamento IP de instâncias .....	937
Endereços IPv4 privados e nomes de host DNS internos .....	937
Endereços IPv4 públicos e nomes de host DNS externos .....	938
Endereços IP elásticos (IPv4) .....	939
Servidor DNS da Amazon .....	939
Endereços IPv6 .....	939
Trabalhar com os endereços IPv4 para as instâncias .....	940
Trabalhar com os endereços IPv6 para as instâncias .....	943
Vários endereços IP .....	946
Traga seus próprios endereços IP .....	954
Requisitos e cotas .....	954
Configurar seu intervalo de endereços BYOIP .....	955
Trabalhar com o intervalo de endereços .....	962
Saiba mais .....	963
Atribuição de prefixos .....	963
Noções básicas para atribuição de prefixos .....	964
Considerações e limites para prefixos .....	964
Trabalhar com prefixos .....	964
Endereços IP elásticos .....	975
Definição de preço de endereços IP elásticos .....	975
Noções básicas sobre endereços IP elásticos .....	975
Trabalhar com endereços IP elásticos .....	976
Usar DNS reverso para aplicações de e-mail .....	982
Limite de endereços IP elásticos .....	983
Interfaces de rede .....	984
Conceitos básicos da interface de rede .....	984
Placas de rede .....	986
Endereços IP por interface de rede por tipo de instância .....	986
Trabalhar com interfaces de rede .....	1001
Cenários para interfaces de rede .....	1009
Melhores práticas para configurar interfaces de rede .....	1011
Interfaces de rede gerenciadas pelo solicitante .....	1012
Largura de banda de rede .....	1013
Largura de banda disponível da instância .....	1014
Monitorar largura de banda da instância .....	1015
Redes avançadas .....	1015
Suporte a redes avançadas .....	1016
Habilitar redes avançadas na instância .....	1016
Redes avançadas: ENA .....	1016
Rede avançada: Intel 82599 VF .....	1026
Otimizações do sistema operacional .....	1032
Métricas de performance da rede .....	1032
Solução de problemas do ENA .....	1036
Elastic Fabric Adapter .....	1044
Conceitos básicos de EFA .....	1045
Interfaces e bibliotecas compatíveis .....	1046

Tipos de instâncias compatíveis .....	1046
AMIs compatíveis .....	1046
Limitações de EFA .....	1047
Conceitos básicos do EFA e MPI .....	1047
Conceitos básicos do EFA e NCCL .....	1055
Trabalhar com EFA .....	1078
Monitorar um EFA .....	1081
Verificar o instalador EFA usando uma soma de verificação .....	1082
Grupos de posicionamento .....	1084
Placement groups de cluster .....	1085
Placement groups de partição .....	1086
Placement groups de distribuição .....	1086
Regras e limitações do placement group .....	1087
Criar um placement group .....	1088
Marcar um placement group .....	1089
Executar instâncias em um placement group .....	1092
Descrever instâncias em um placement group .....	1093
Alterar o placement group de uma instância .....	1094
Excluir um placement group .....	1095
Conexão MTU .....	1096
Frames jumbo (9.001 MTU) .....	1097
Path MTU Discovery .....	1098
Verificar o MTU do caminho entre dois hosts .....	1098
Verificar e definir o MTU na instância do Linux .....	1099
Troubleshoot .....	1100
Nuvens privadas virtuais .....	1100
Documentação da Amazon VPC .....	1100
EC2-Classic .....	1100
Detectar plataformas suportadas .....	1101
Tipos de instância disponíveis no EC2-Classic .....	1102
Diferenças entre instâncias no EC2-Classic e em uma VPC .....	1103
Compartilhar e acessar recursos entre EC2-Classic e uma VPC .....	1107
ClassicLink .....	1109
Migre do EC2-Classic para uma VPC .....	1120
Segurança .....	1130
Segurança da infraestrutura .....	1130
Isolamento de rede .....	1131
Isolamento em hosts físicos .....	1131
Controlar o tráfego de rede .....	1131
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 .....	1136
Acesso à rede para a instância .....	1137
Atributos de permissões do Amazon EC2 .....	1137
IAM e Amazon EC2 .....	1137
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 .....	1212
Etiquetar uma chave pública .....	1213
Recuperar a chave pública da chave privada .....	1215
Recuperar a chave pública por meio de metadados de instância .....	1216
Localizar a chave pública em uma instância .....	1216
Identificar o par de chaves que foi especificado na execução .....	1217
Verificar a impressão digital do par de chaves .....	1217
Adicionar ou substituir um par de chaves na sua instância .....	1218
Excluir o par de chaves .....	1219
Excluir uma chave pública de uma instância .....	1220
Conectar-se à instância do Linux em caso de perda da chave privada .....	1220
Grupos de segurança .....	1225
Regras de grupos de segurança .....	1226
Acompanhamento da conexão .....	1227
Grupos de segurança padrão e personalizados .....	1229
Trabalhar com grupos de segurança .....	1230
Regras de grupo de segurança para diferentes casos de uso .....	1240
Gerenciamento de atualizações .....	1246
Validação de conformidade .....	1246
Storage .....	1247
Amazon EBS .....	1248
Recursos do Amazon EBS .....	1249
Volumes do EBS .....	1250
Snapshots do EBS .....	1303
Amazon Data Lifecycle Manager .....	1359
Serviços de dados do EBS .....	1405
Volumes do EBS e NVMe .....	1434
Otimização de EBS .....	1438
Performance do EBS .....	1460
Métricas do CloudWatch para o EBS .....	1477
CloudWatch Events para EBS .....	1484
Cotas do EBS .....	1494
Armazenamento de instâncias .....	1494
Vida útil do armazenamento de instâncias .....	1495
Volumes de armazenamento de instâncias .....	1496
Adicionar volumes de armazenamento de instâncias .....	1504
Volumes de armazenamento de instâncias SSD .....	1508
Volumes de troca de armazenamento de instâncias .....	1510
Otimizar a performance dos discos .....	1512
Armazenamento de arquivos .....	1513
Amazon S3 .....	1514
Amazon EFS .....	1515
Limites de volumes de instância .....	1520
Limites de volumes do Sistema Nitro .....	1520
Limites de volumes específicos do Linux .....	1521
Largura de banda x capacidade .....	1521
Volume do dispositivo raiz .....	1521
Conceitos de armazenamento do dispositivo raiz .....	1522
Escolher uma AMI por tipo de dispositivo raiz .....	1523
Determinar o tipo de dispositivo raiz da instância .....	1524
Alterar o volume raiz para persistir .....	1525
Alterar o tamanho inicial do volume raiz .....	1528
Nomes de dispositivos .....	1528
Nomes de dispositivos disponíveis .....	1529
Considerações sobre nomes de dispositivos .....	1530
Mapeamentos de dispositivos de blocos .....	1530

Conceitos de mapeamento de dispositivos de blocos .....	1531
Mapeamento de dispositivos de blocos da AMI .....	1534
Mapeamento de dispositivos de blocos de instância .....	1536
Recursos e tags .....	1542
Localizações de recursos .....	1542
IDs de recursos .....	1543
Listar e filtrar seus recursos .....	1544
Listar e filtrar recursos usando o console .....	1545
Listar e filtrar usando a CLI e a API .....	1549
Listar e filtrar recursos entre Regiões usando o Amazon EC2 Global View .....	1551
Marcar com tag os recursos do .....	1552
Conceitos básicos de tags .....	1552
Marcar com tag os recursos do .....	1553
Restrições de tags .....	1556
Gerenciamento de tags e acesso .....	1557
Marcar com tag recursos para faturamento .....	1557
Trabalhar com tags usando o console .....	1558
Trabalhar com tags usando a linha de comando .....	1561
Adicionar tags a um recurso usando o CloudFormation .....	1564
Cotas de serviço .....	1565
Visualizar os limites atuais .....	1565
Solicitar um aumento .....	1566
Restrição para e-mails enviados usando a porta 25 .....	1566
Relatórios de uso .....	1567
Solução de problemas .....	1568
Solucionar problemas de execução .....	1568
Limite de instâncias excedido .....	1568
Capacidade insuficiente da instância .....	1569
A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis. ....	1569
A instância é encerrada imediatamente .....	1570
Conecte-se à sua instância .....	1571
Causas comuns de problemas de conexão .....	1571
Erro ao se conectar à sua instância: limite de tempo da conexão atingido .....	1572
Erro: não foi possível carregar a chave ... Esperando: QUALQUER CHAVE PRIVADA .....	1576
Erro: Chave do usuário não reconhecida pelo servidor .....	1576
Erro: permissão negada ou conexão fechada pela porta 22 de [instância] .....	1577
Erro: arquivo de chave privada desprotegido .....	1579
Erro: a chave privada deve começar com "----BEGIN RSA PRIVATE KEY----" e terminar com "----END RSA PRIVATE KEY----" .....	1580
Erro: o servidor recusou nossa chave ou não há métodos de autenticação compatíveis disponíveis .....	1580
Não é possível fazer o ping da instância .....	1581
Erro: Server unexpectedly closed network connection (A conexão de rede foi fechada inesperadamente pelo servidor) .....	1581
Erro: falha na validação da chave do host para EC2 Instance Connect .....	1581
Parar a instância .....	1583
Forçar a parada da instância .....	1583
Para criar uma instância de substituição .....	1584
Encerrar a instância .....	1585
A instância é encerrada imediatamente .....	1586
Encerramento atrasado da instância .....	1586
Instância encerrada ainda sendo exibida .....	1586
Instâncias executadas ou encerradas automaticamente .....	1586
Falha nas verificações de status .....	1586
Analizar informações de verificação de status .....	1587
Recuperar os logs do sistema .....	1588

Solução de problemas de erros de logs do sistema para instâncias baseadas em Linux .....	1588
Sem memória: encerrar processo .....	1589
ERRO: falha em mmu_update (falha na atualização do gerenciamento de memória) .....	1590
Erro de E/S (falha de dispositivo de blocos) .....	1591
ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado) .....	1592
request_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux) .....	1593
"FATAL: kernel antigo demais" e "fsck: Não existe esse arquivo ou diretório ao tentar abrir / dev" (falta de correspondência entre o kernel e a AMI) .....	1594
"FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes) .....	1594
ERRO Kernel inválido (kernel incompatível com EC2) .....	1595
fsck: Nenhum arquivo ou diretório ao tentar abrir... (Sistema de arquivos não encontrado) .....	1596
Erro geral ao montar os sistemas de arquivos (falha na montagem) .....	1598
VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz) .....	1599
Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz) .....	1600
XENBUS: Dispositivo sem driver... .....	1601
...dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos) .....	1602
O fsck morreu com status de saída... (Dispositivo ausente) .....	1603
Prompt do GRUB (grubdom>) .....	1604
Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded) .....	1606
Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux) .....	1607
XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus) ..	1608
Solucionar problemas de uma instância não acessível .....	1609
Reinicialização da instância .....	1609
Saída do console da instância .....	1609
Fazer uma captura de tela de uma instância inacessível .....	1610
Recuperação da instância quando um computador host falhar .....	1611
Inicialização a partir do volume errado .....	1612
EC2Rescue for Linux .....	1613
Instalar o EC2Rescue para Linux .....	1613
(Opcional) Verifique a assinatura de EC2Rescue para Linux .....	1614
Trabalhar com EC2Rescue para Linux .....	1617
Desenvolver módulos do EC2Rescue .....	1619
Console serial do EC2 .....	1623
Configurar o acesso ao console serial do EC2 .....	1624
Conectar-se ao console serial do EC2 .....	1629
Encerrar uma sessão do console serial do EC2 .....	1634
Solucionar problemas da instância usando o console Serial do EC2 .....	1635
Enviar uma interrupção para diagnóstico .....	1640
Tipos de instâncias compatíveis .....	1641
Prerequisites .....	1641
Enviar uma interrupção para diagnóstico .....	1643
Histórico do documento .....	1645
História dos anos anteriores .....	1655

# 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](#).

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. \(p. 5\)](#)
- [Tutorial: Comece a usar instâncias Linux do Amazon EC2 \(p. 9\)](#)

## Basics

- [Instâncias e AMIs \(p. 200\)](#)
- [Regiões e zonas \(p. 923\)](#)
- [Tipos de instância \(p. 203\)](#)
- [Tags \(p. 1552\)](#)

## Redes e segurança

- [Pares de chaves \(p. 1209\)](#)
- [Grupos de segurança \(p. 1225\)](#)
- [Endereços IP elásticos \(p. 975\)](#)
- [Nuvens privadas virtuais \(p. 1100\)](#)

## Storage

- [Amazon EBS \(p. 1248\)](#)
- [Armazenamento de instâncias \(p. 1494\)](#)

## Trabalhar com instâncias do Linux

- [AWS Systems Manager Run Command \(Run Command do AWS Systems Manager\) no AWS Systems Manager User Guide \(Guia do usuário do AWS Systems Manager\).](#)
- [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 15\)](#)
- [Tutorial: configurar o SSL/TLS no Amazon Linux 2 \(p. 25\)](#)

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) da

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 segundo, 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 \(p. 5\)](#)
2. [Criar um par de chaves \(p. 5\)](#)
3. [Crie um grupo de segurança \(p. 6\)](#)

Quando terminar, você estará pronto para o tutorial [Conceitos básicos do Amazon EC2 \(p. 9\)](#).

## 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. Uma instância do Linux não tem senha; você usa um par de chaves para fazer logon na instância com segurança. Você especifica o nome do par de chaves ao iniciar a instância e fornece a chave privada ao fazer logon usando SSH.

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 \(p. 923\)](#).

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.

9. Se você usar um cliente SSH em um computador macOS ou Linux para conectar-se à instância do Linux, use o seguinte comando para definir as permissões do arquivo de chave privada de maneira que apenas você possa lê-lo.

```
chmod 400 my-key-pair.pem
```

Se você não definir essas permissões, não poderá conectar-se à instância usando esse par de chaves. Para obter mais informações, consulte [Erro: arquivo de chave privada desprotegido \(p. 1579\)](#).

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

## 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 SSH. 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 \(p. 923\)](#).

#### 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 \(p. 1240\)](#).
  - 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 SSH. 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 SSH. 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 SSH 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 SSH 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 Linux \(p. 1225\)](#).

# Tutorial: Comece a usar instâncias Linux 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 Linux. 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

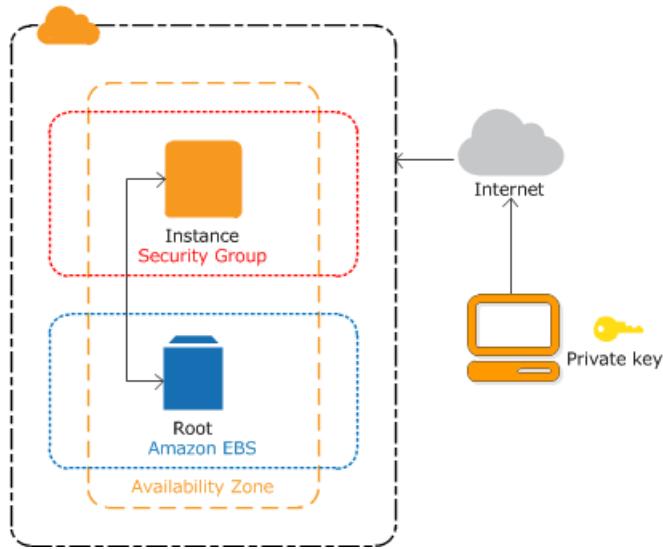
- [Overview \(p. 9\)](#)
- [Prerequisites \(p. 10\)](#)
- [Etapa 1: executar uma instância \(p. 10\)](#)
- [Etapa 2: conectar-se à instância \(p. 11\)](#)
- [Etapa 3: limpar a instância \(p. 11\)](#)
- [Próximas etapas \(p. 12\)](#)

## Tutoriais relacionados

- Se você preferir executar uma instância Windows, consulte este tutorial no Guia do usuário do Amazon EC2 para instâncias do Windows: [Conceitos básicos das instâncias Windows 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. \(p. 5\)](#).

## Etapa 1: executar uma instância

Você pode executar uma instância Linux 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. \(p. 510\)](#). Para obter informações sobre outras formas de executar sua instância, consulte [Executar sua instância \(p. 509\)](#).

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 uma versão HVM do Amazon Linux 2. 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

Há várias formas de conectar-se a sua instância do Linux. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).

**Important**

Não é possível conectar-se à instância a menos que você a tenha executado com um par de chaves, para o qual existe o arquivo .pem, e a tenha executado com um grupo de segurança que permita acesso SSH em seu computador. Se você não puder se conectar à sua instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#) para obter assistência.

## 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 \(p. 12\)](#).

**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 \(p. 562\)](#).

#### 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. \(p. 1274\)](#) e [Vincular um volume de Amazon EBS a uma instância \(p. 1277\)](#).
- Instale a pilha LAMP. Para obter mais informações, consulte [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 15\)](#).

# Melhores práticas do Amazon EC2

Esta lista de práticas ajudará você a obter o máximo benefício do Amazon EC2.

## Security

- Gerencie o acesso aos recursos e às APIs da AWS usando a federação de identidades, os usuários do IAM e as funções do IAM. Estabeleça políticas e procedimentos de gerenciamento de credenciais para criar, distribuir, rotacionar e revogar credenciais de acesso da AWS. Para obter mais informações, consulte [Melhores práticas do IAM](#) no Guia do usuário do IAM.
- Implemente as regras menos permissivas para o security group. Para obter mais informações, consulte [Regras de grupos de segurança \(p. 1226\)](#).
- Corrija, atualize e proteja regularmente o sistema operacional e os aplicativos em sua instância. Para obter mais informações sobre como atualizar o Amazon Linux 2 ou a Amazon Linux AMI, consulte [Como gerenciar o software na instância Linux](#) no Guia do usuário do Amazon EC2 para instâncias do Linux.

## Storage

- Compreenda as implicações do tipo de dispositivo raiz para a persistência, o backup e a recuperação de dados. Para obter mais informações, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#).
- 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 \(p. 591\)](#).
- 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 \(p. 1418\)](#).

## 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 \(p. 649\)](#) e [Marcar com tag os recursos do Amazon EC2 \(p. 1552\)](#).
- 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 \(p. 1565\)](#).

## Backup e recuperação

- Faça backup de seus volumes do EBS regularmente usando [Snapshots do Amazon EBS \(p. 1303\)](#) e crie uma [Imagen de máquina da Amazon \(AMI\) \(p. 72\)](#) 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 \(p. 937\)](#).

- Monitorar e responder a eventos. Para obter mais informações, consulte [Monitorar o Amazon EC2 \(p. 838\)](#).
- 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 \(p. 984\)](#). 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.

# Tutoriais para instâncias do Amazon EC2 que executam no Linux

Os tutoriais a seguir mostram como executar tarefas comuns usando instâncias do EC2 que executam o Linux. A AWS fornece o Amazon Linux 2 e a AMI do Amazon Linux. Para obter mais informações, consulte [Amazon Linux 2](#) e [Amazon Linux AMI](#). Para acessar tutoriais em vídeo, consulte [AWS Instructional Videos and Labs](#) (Vídeos explicativos e laboratórios da AWS).

## Tutoriais

- [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 15\)](#)
- [Tutorial: configurar o SSL/TLS no Amazon Linux 2 \(p. 25\)](#)
- [Tutorial: Hospedar um blog do WordPress no Amazon Linux 2 \(p. 40\)](#)
- [Tutorial: Instalar um servidor web LAMP no Amazon Linux AMI \(p. 50\)](#)
- [Tutorial: Configurar o SSL/TLS com a AMI do Amazon Linux \(p. 60\)](#)

## Tutorial: Instalar um servidor web LAMP no Amazon Linux 2

Os procedimentos a seguir ajudam a instalar um servidor web Apache com suporte para PHP e [MariaDB](#) (um fork desenvolvido pela comunidade de MySQL) em sua instância do Amazon Linux 2 (às vezes denominado servidor web LAMP ou pilha LAMP). Você pode usar esse servidor para hospedar um site estático ou para implantar um aplicativo PHP dinâmico que lê e grava informações em um banco de dados.

### Important

Se você estiver tentando configurar um servidor web LAMP em uma distribuição diferente, como Ubuntu ou Red Hat Enterprise Linux, este tutorial não funcionará. Para Amazon Linux AMI, consulte [Tutorial: Instalar um servidor web LAMP no Amazon Linux AMI \(p. 50\)](#). Para o Ubuntu, consulte a seguinte documentação da comunidade do Ubuntu: [ApacheMySQLPHP](#). Para outras distribuições, consulte a documentação específica.

Opção: concluir este tutorial usando a automação

Para concluir este tutorial usando a automação do AWS Systems Manager em vez das tarefas a seguir, execute o documento de automação [Docs-InstallALAMPServer-AL2 da AWS](#).

## Tarefas

- [Etapa 1: Preparar o servidor LAMP \(p. 16\)](#)
- [Etapa 2: Testar o servidor LAMP \(p. 19\)](#)
- [Etapa 3: Proteger o servidor do banco de dados \(p. 20\)](#)
- [Etapa 4: \(opcional\) instalar o phpMyAdmin \(p. 21\)](#)
- [Troubleshoot \(p. 24\)](#)

- [Tópicos relacionados \(p. 24\)](#)

## Etapa 1: Preparar o servidor LAMP

### Prerequisites

- Este tutorial pressupõe que você já tenha executado uma nova instância usando o Amazon Linux 2, com um nome DNS público acessível pela Internet. Para obter mais informações, consulte [Etapa 1: executar uma instância \(p. 10\)](#). Você também precisa ter configurado o security group para permitir conexões SSH (porta 22), HTTP (porta 80) e HTTPS (porta 443). Para obter mais informações sobre esses pré-requisitos, consulte [Autorizar tráfego de entrada para suas instâncias do Linux \(p. 1205\)](#).
- O procedimento a seguir instala a versão mais recente de PHP disponível no Amazon Linux 2, atualmente PHP 7.2. Se você planeja usar aplicativos PHP diferentes daqueles descritos neste tutorial, você deve verificar a compatibilidade com o PHP 7.2.

### Para preparar o servidor LAMP

1. [Conecte-se à sua instância \(p. 11\)](#).
2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. Esse processo pode levar alguns minutos, mas é importante ter certeza de que você tem as atualizações de segurança e correções de bug mais recentes.

A opção `-y` instala as atualizações sem solicitar confirmação. Para examinar as atualizações antes da instalação, você pode omitir essa opção.

```
[ec2-user ~]$ sudo yum update -y
```

3. Instale os repositórios de extras `lamp-mariadb10.2-php7.2` e `php7.2` do Amazon Linux para obter as versões mais recentes dos pacotes de LAMP MariaDB e de PHP para o Amazon Linux 2.

```
[ec2-user ~]$ sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
```

Se receber um erro relatando `sudo: amazon-linux-extras: command not found`, isso significa que sua instância não foi executada com uma AMI do Amazon Linux 2 (talvez você esteja usando a Amazon Linux AMI). Você pode visualizar sua versão do Amazon Linux usando o comando a seguir.

```
cat /etc/system-release
```

Para configurar um servidor web LAMP na Amazon Linux AMI, consulte [Tutorial: Instalar um servidor web LAMP no Amazon Linux AMI \(p. 50\)](#).

4. Agora que sua instância é atual, você pode instalar o servidor web Apache, o MariaDB e os pacotes de software do PHP.

Use o comando `yum install` para instalar os vários pacotes de software e todas as dependências relacionadas ao mesmo tempo.

```
[ec2-user ~]$ sudo yum install -y httpd mariadb-server
```

Você pode visualizar as versões atuais desses pacotes usando o comando a seguir:

```
yum info package_name
```

5. Inicie o servidor web Apache.

```
[ec2-user ~]$ sudo systemctl start httpd
```

6. Use o comando systemctl para configurar o servidor web Apache para iniciar em cada inicialização do sistema.

```
[ec2-user ~]$ sudo systemctl enable httpd
```

Você pode verificar se httpd está ativo executando o seguinte comando:

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

7. Adicione uma regra de segurança para permitir conexões HTTP de entrada (porta 80) na instância caso você ainda não tenha feito isso. Por padrão, um grupo de segurança launch-wizard-N foi configurado para a instância durante a inicialização. Esse grupo contém uma única regra para permitir conexões SSH.

- a. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
- b. Escolha Instances (Instâncias) e selecione a instância.
- c. Na guia Security (Segurança), exiba as regras de entrada. Você deve ver a seguinte regra:

Port range	Protocol	Source
22	tcp	0.0.0.0/0

#### Warning

Usar 0.0.0.0/0 permite que todos os endereços IPv4 acessem sua instância usando o SSH. 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.

- d. Escolha o link do grupo de segurança. Usando os procedimentos contidos em [Adicionar regras a um grupo de segurança \(p. 1233\)](#), adicione uma nova regra de segurança de entrada com os seguintes valores:
  - Type (Tipo): HTTP
  - Protocol (Protocolo): TCP
  - Port Range: 80
  - Source (Origem): personalizado
8. Teste o servidor web. Em um navegador, digite o endereço DNS público (ou o endereço IP público) de sua instância. Se não houver conteúdo em /var/www/html, você deverá verificar a página de teste do Apache. Você pode obter o DNS público da instância usando o console do Amazon EC2 (verifique a coluna Public DNS (DNS público)). Se essa coluna estiver oculta, escolha Show/Hide Columns (Mostrar/ocultar colunas) (o ícone em forma de engrenagem) e escolha Public DNS (DNS público)).

Verifique se o grupo de segurança da instância contém uma regra para permitir o tráfego HTTP na porta 80. Para obter mais informações, consulte [Adicionar regras a um grupo de segurança \(p. 1233\)](#).

#### Important

Se você não estiver usando o Amazon Linux, poderá ser necessário configurar o firewall na instância para permitir essas conexões. Para obter mais informações sobre como configurar o firewall, consulte a documentação de sua distribuição específica.

## Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

### If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting [www.example.com](http://www.example.com), you should send e-mail to "webmaster@example.com".

### If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the image below on web sites powered by the Apache HTTP Server:



2.4

O httpd do Apache é usado para os arquivos que são mantidos em um diretório chamado raiz de documentos do Apache. O diretório raiz de documentos Apache do Amazon Linux é `/var/www/html`, que, por padrão, é de propriedade da raiz.

Para permitir que a conta do `ec2-user` manipule arquivos nesse diretório, você deve modificar a propriedade e as permissões do diretório. Existem diversas maneiras de realizar essa tarefa. Neste tutorial, você adiciona o usuário `ec2-user` ao grupo `apache` para dar ao grupo `apache` a propriedade do diretório `/var/www` e atribuir permissões de gravação ao grupo.

Para definir permissões de arquivo

1. Adicione o usuário (neste caso, o `ec2-user`) ao grupo do `apache`.

```
[ec2-user ~]$ sudo usermod -a -G apache ec2-user
```

2. Faça logout e login novamente para selecionar o novo grupo verifique sua associação.

- a. Faça logout (use o comando `exit` ou feche a janela do terminal):

```
[ec2-user ~]$ exit
```

- b. Para verificar sua associação no grupo `apache`, reconecte-se à instância e execute o comando a seguir:

```
[ec2-user ~]$ groups
ec2-user adm wheel apache systemd-journal
```

3. Altere a propriedade do grupo do `/var/www` e seu conteúdo para o grupo do `apache`.

```
[ec2-user ~]$ sudo chown -R ec2-user:apache /var/www
```

4. Para adicionar as permissões de gravação do grupo e definir o ID do grupo nos subdiretórios futuros, altere as permissões de diretório de `/var/www` e de seus subdiretórios.

```
[ec2-user ~]$ sudo chmod 2775 /var/www && find /var/www -type d -exec sudo chmod 2775 {} \;
```

5. Para adicionar permissões de gravação do grupo, altere recursivamente as permissões de arquivo de /var/www e de seus subdiretórios:

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
```

Agora, ec2-user (e outros todos os futuros do grupo apache) poderão adicionar, excluir e editar arquivos na raiz do documento Apache, permitindo que você adicione conteúdo, como um site estático ou um aplicativo PHP.

Para proteger o servidor web (opcional)

Um servidor web que executa o protocolo HTTP não fornece nenhuma segurança de transporte para os dados que envia ou recebe. Quando você se conecta a um servidor HTTP usando um navegador da web, as URLs que você acessa, o conteúdo de páginas da web recebido e o conteúdo (incluindo senhas) de todos os formulários HTML enviado por você ficam visíveis para os espiões em qualquer ponto da rede. A melhor prática para proteger o servidor web é instalar suporte para HTTPS (HTTP seguro), que protege os dados por meio de criptografia SSL/TLS.

Para obter informações sobre como habilitar o HTTPS no servidor, consulte [Tutorial: configurar o SSL/TLS no Amazon Linux 2 \(p. 25\)](#).

## Etapa 2: Testar o servidor LAMP

Se o servidor estiver instalado e em execução, e suas permissões de arquivo estiverem definidas corretamente, a conta do ec2-user poderá criar um arquivo PHP no diretório /var/www/html disponível na Internet.

Para testar o servidor do LAMP

1. Crie um arquivo PHP no diretório base do Apache.

```
[ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Se você receber o erro "Permissão negada" ao tentar executar esse comando, tente fazer logout e login novamente para obter as permissões corretas do grupo que você configurou em [Para definir permissões de arquivo \(p. 18\)](#).

2. Em um navegador da web, digite a URL do arquivo que você acabou de criar. Essa URL é o endereço DNS público da instância seguido por uma barra e o nome do arquivo. Por exemplo:

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Você deve ver a página de informações do PHP:

PHP Version 7.2.0	
System	Linux ip-172-31-22-15.us-west-2.compute.internal 4.9.62-10.57.amzn2.x86_64 #1 SMP Wed Dec 6 00:07:49 UTC 2017 x86_64
Build Date	Dec 13 2017 03:34:37
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mysqlind.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API20170718,NTS
PHP Extension Build	API20170718,NTS

Se você não vir essa página, verifique se o arquivo `/var/www/html/phpinfo.php` foi criado corretamente na etapa anterior. Você também pode verificar se todos os pacotes necessários foram instalados com o comando a seguir.

```
[ec2-user ~]$ sudo yum list installed httpd mariadb-server php-mysqlnd
```

Se alguns dos pacotes necessários não estiverem listados na saída, instale-os com o comando `sudo yum install package`. Além disso, verifique se os extras `php7.2` e `lamp-mariadb10.2-php7.2` estão habilitados na saída do comando `amazon-linux-extras`.

3. Exclua o arquivo `phpinfo.php`. Embora essas informações possam ser úteis, elas não devem ser transmitidas pela Internet por motivos de segurança.

```
[ec2-user ~]$ rm /var/www/html/phpinfo.php
```

Agora você deve ter um servidor web do LAMP totalmente funcional. Se adicionar conteúdo ao diretório base do Apache em `/var/www/html`, você deverá poder visualizar esse conteúdo no endereço DNS público de sua instância.

## Etapa 3: Proteger o servidor do banco de dados

A instalação padrão do servidor MariaDB tem vários recursos que são bons para teste e desenvolvimento, mas devem ser desabilitados ou removidos em servidores de produção. O comando `mysql_secure_installation` orienta você durante o processo de configuração de uma senha raiz e da remoção de recursos não seguros da instalação. Mesmo que você não esteja planejando usar o servidor MariaDB é recomendável executar este procedimento.

Para proteger o servidor MariaDB

1. Inicie o servidor MariaDB.

```
[ec2-user ~]$ sudo systemctl start mariadb
```

2. Executar `mysql_secure_installation`.

```
[ec2-user ~]$ sudo mysql_secure_installation
```

- a. Quando solicitado, digite uma senha para a conta raiz.
  - i. Digite a senha raiz atual. Por padrão, a conta raiz não tem uma senha definida. Pressione Enter.
  - ii. Digite **Y** para definir uma senha e digite uma senha segura duas vezes. Para obter mais informações sobre como criar uma senha segura, consulte <https://identitysafe.norton.com/password-generator/>. Armazene essa senha em um lugar seguro.

A configuração de uma senha raiz para o MariaDB é somente a medida mais básica para proteger seu banco de dados. Ao criar ou instalar um aplicativo controlado por banco de dados, geralmente, você cria um usuário de serviço de banco para esse aplicativo e evita usar a conta raiz para qualquer coisa que não seja a administração do banco de dados.

- b. Digite **Y** para remover as contas de usuários anônimos.
- c. Digite **Y** para desabilitar o recurso de login remoto da raiz.
- d. Digite **Y** para remover o banco de dados de teste.
- e. Digite **Y** para recarregar as tabelas de privilégios e salvar suas alterações.
3. (Opcional) Se você não pretende usar o servidor MariaDB imediatamente, interrompa-o. Você poderá reiniciá-lo quando precisar dele novamente.

```
[ec2-user ~]$ sudo systemctl stop mariadb
```

4. (Opcional) Se você quiser que o servidor MariaDB seja iniciado a cada inicialização, digite o comando a seguir.

```
[ec2-user ~]$ sudo systemctl enable mariadb
```

## Etapa 4: (opcional) instalar o phpMyAdmin

O [phpMyAdmin](#) é uma ferramenta de gerenciamento de banco de dados baseada na web que você pode usar para visualizar e editar os bancos de dados MySQL na instância do EC2. Siga as etapas a seguir para instalar e configurar o [phpMyAdmin](#) em sua instância do Amazon Linux.

### Important

Não recomendamos usar o [phpMyAdmin](#) para acessar um servidor LAMP, a menos que você tenha habilitado o SSL/TLS no Apache. Caso contrário, sua senha de administrador de banco de dados e outros dados serão transmitidos de forma desprotegida pela Internet. Para ver as recomendações de segurança dos desenvolvedores, consulte [Securing your phpMyAdmin installation](#). Para obter informações gerais sobre como proteger um servidor web em uma instância do EC2, consulte [Tutorial: configurar o SSL/TLS no Amazon Linux 2 \(p. 25\)](#).

### Para instalar o phpMyAdmin

1. Instale as dependências necessárias.

```
[ec2-user ~]$ sudo yum install php-mbstring php-xml -y
```

2. Reinicie o Apache.

```
[ec2-user ~]$ sudo systemctl restart httpd
```

3. Reinicie php-fpm.

```
[ec2-user ~]$ sudo systemctl restart php-fpm
```

- Navegue até o diretório base do Apache em /var/www/html.

```
[ec2-user ~]$ cd /var/www/html
```

- Selecione um pacote de origem para a versão mais recente do phpMyAdmin em <https://www.phpmyadmin.net/downloads>. Para fazer download do arquivo diretamente para a instância, copie o link e cole-o em um comando wget, como neste exemplo:

```
[ec2-user html]$ wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz
```

- Crie uma pasta phpMyAdmin e extraia o pacote dela com o comando a seguir.

```
[ec2-user html]$ mkdir phpMyAdmin && tar -xvzf phpMyAdmin-latest-all-languages.tar.gz -C phpMyAdmin --strip-components 1
```

- Exclua o tarball *phpMyAdmin-latest-all-languages.tar.gz*.

```
[ec2-user html]$ rm phpMyAdmin-latest-all-languages.tar.gz
```

- (Opcional) Se o servidor MySQL não estiver em execução, inicie-o agora.

```
[ec2-user ~]$ sudo systemctl start mariadb
```

- Em um navegador da web, digite a URL da instalação do phpMyAdmin. Essa URL é o endereço DNS público (ou o endereço IP público) da instância seguido por uma barra e o nome do diretório de instalação. Por exemplo:

```
http://my.public.dns.amazonaws.com/phpMyAdmin
```

Você deve ver a página de login do phpMyAdmin:



10. Inicie a sessão na instalação do phpMyAdmin com o nome de usuário `root` e a senha raiz do MySQL criada anteriormente.

A instalação ainda deve ser configurada antes que você a coloque em serviço. Sugerimos que você comece criando manualmente o arquivo de configuração, da seguinte maneira:

- a. Para começar com um arquivo de configuração mínima, use seu editor de texto favorito para criar um novo arquivo e, em seguida, copie o conteúdo de `config.sample.inc.php` para ele.

- b. Salve o arquivo como config.inc.php no diretório do phpMyAdmin que contém index.php.
- c. Consulte as instruções posteriores à criação dos arquivos na seção [Como usar o script de configuração](#) das instruções de instalação do phpMyAdmin para qualquer configuração adicional.

Para obter informações sobre o uso do phpMyAdmin, consulte o [Guia do usuário do phpMyAdmin](#).

## Troubleshoot

Esta seção oferece sugestões para resolver problemas comuns que você pode encontrar ao configurar um novo servidor do LAMP.

### Não consigo me conectar ao servidor usando um navegador da web

Execute as seguintes verificações para ver se o servidor da web do Apache está em execução e acessível.

- O servidor web está em execução?

Você pode verificar se httpd está ativo executando o seguinte comando:

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

Se o processo httpd não estiver em execução, repita as etapas descritas em [Para preparar o servidor LAMP \(p. 16\)](#).

- O firewall está configurado corretamente?

Verifique se o grupo de segurança da instância contém uma regra para permitir o tráfego HTTP na porta 80. Para obter mais informações, consulte [Adicionar regras a um grupo de segurança \(p. 1233\)](#).

### Não consigo me conectar ao meu servidor usando HTTPS

Execute as seguintes verificações para ver se o servidor da web do Apache está configurado para dar suporte a HTTPS.

- O servidor Web está configurado corretamente?

Depois de instalar o Apache, o servidor é configurado para tráfego HTTP. Para suportar HTTPS, ative o TLS no servidor e instale um certificado SSL. Para obter mais informações, consulte [Tutorial: configurar o SSL/TLS no Amazon Linux 2 \(p. 25\)](#).

- O firewall está configurado corretamente?

Verifique se o grupo de segurança da instância contém uma regra para permitir o tráfego HTTPS na porta 443. Para obter mais informações, consulte [Adicionar regras a um grupo de segurança \(p. 1233\)](#).

## Tópicos relacionados

Para obter mais informações sobre como transferir arquivos para a instância ou como instalar um blog do WordPress no servidor web, consulte a documentação a seguir:

- [Transferir arquivos para sua instância do Linux usando WinSCP \(p. 555\)](#)
- [Transfira arquivos para instâncias do Linux usando um cliente SCP \(p. 539\)](#)

- [Tutorial: Hospedar um blog do WordPress no Amazon Linux 2 \(p. 40\)](#)

Para obter mais informações sobre os comandos e o software usados neste tutorial, consulte as seguintes páginas da web:

- Servidor web Apache: <http://httpd.apache.org/>
- Servidor de banco de dados MariaDB: <https://mariadb.org/>
- Linguagem de programação PHP: <http://php.net/>
- O comando chmod: <https://en.wikipedia.org/wiki/Chmod>
- O comando chown: <https://en.wikipedia.org/wiki/Chown>

Para obter mais informações sobre como registrar um nome de domínio para o servidor web ou transferir um nome de domínio existente para este host, consulte [Como criar e migrar domínios e subdomínios para o Amazon Route 53](#) no Guia do desenvolvedor do Amazon Route 53.

## Tutorial: configurar o SSL/TLS no Amazon Linux 2

O Secure Sockets Layer/Transport Layer Security (SSL/TLS) cria um canal criptografado entre um servidor Web e um cliente Web que protege os dados em trânsito contra espionagem. Este tutorial explica como adicionar suporte manualmente para SSL/TLS em uma instância do EC2 com o Amazon Linux 2 e o servidor Web do Apache. Este tutorial pressupõe que você não esteja usando um平衡ador de carga. Se você estiver usando Elastic Load Balancing, poderá optar por configurar o descarregamento do SSL no balanceador de carga, usando, em vez disso, um certificado do [AWS Certificate Manager](#).

Por motivos históricos, a criptografia na Web é conhecida simplesmente como SSL. Embora os navegadores da Web ainda ofereçam suporte ao SSL, o protocolo sucessor, o TLS, é menos vulnerável a ataques. O Amazon Linux 2 desativa o suporte no lado do servidor para todas as versões do SSL por padrão. Os [órgãos de normas de segurança](#) consideram o TLS 1.0 inseguro, e tanto o TLS 1.0 quanto o TLS 1.1 estão prestes a ser formalmente [suspenso](#)s pelo IETF. Este tutorial contém orientações baseadas exclusivamente na ativação do TLS 1.2. (Existe um protocolo TLS 1.3 mais recente, mas ele não é instalado por padrão no Amazon Linux 2.) Para obter mais informações sobre os padrões de criptografia atualizados, consulte [RFC 7568](#) e [RFC 8446](#).

Este tutorial refere-se à criptografia da Web moderna simplesmente como TLS.

### Important

Esses procedimentos são destinados ao Amazon Linux 2. Também supomos que você esteja começando com uma nova instância do Amazon EC2. Se você estiver tentando configurar uma instância do EC2 executando uma distribuição diferente ou uma instância executando uma versão antiga do Amazon Linux 2, alguns procedimentos deste tutorial poderão não funcionar. Para o Amazon Linux AMI, consulte [Tutorial: Configurar o SSL/TLS com a AMI do Amazon Linux \(p. 60\)](#). Para o Ubuntu, consulte a seguinte documentação da comunidade do Ubuntu: [ApacheMySQLPHP](#). Para o Red Hat Enterprise Linux, consulte: [Como configurar o Servidor Web Apache HTTP](#). Para outras distribuições, consulte a documentação específica.

### Tópicos

- [Prerequisites \(p. 26\)](#)
- [Etapa 1: habilitar o TLS no servidor \(p. 26\)](#)
- [Etapa 2: obter um certificado assinado por uma CA \(p. 28\)](#)
- [Etapa 3: testar e intensificar a configuração de segurança \(p. 33\)](#)
- [Troubleshoot \(p. 36\)](#)

- Automação de certificados: Let's Encrypt com o Certbot no Amazon Linux 2 (p. 36)

## Prerequisites

Antes de começar este tutorial, conclua as seguintes etapas:

- Execute uma instância do Amazon Linux 2 baseada em EBS. Para obter mais informações, consulte [Etapa 1: executar uma instância \(p. 10\)](#).
- Configure seus grupos de segurança para permitir que sua instância aceite conexões nas seguintes portas TCP:
  - SSH (porta 22)
  - HTTP (porta 80)
  - HTTPS (porta 443)

Para obter mais informações, consulte [Autorizar tráfego de entrada para suas instâncias do Linux \(p. 1205\)](#).

- Instale o servidor da Web Apache. Para obter instruções passo a passo, consulte [Tutorial: Instalar um servidor Web LAMP no Amazon Linux 2 \(p. 15\)](#). Somente o pacote httpd e suas dependências são necessários e, portanto, você pode ignorar as instruções que envolvem PHP e MariaDB.
- Para identificar e autenticar sites, a infraestrutura de chave pública (PKI) do TLS depende do Sistema de Nomes de Domínio (DNS). Para usar sua instância do EC2 para hospedar um site público, você precisará registrar um nome de domínio para seu servidor da Web ou transferir um nome de domínio existente para o host do Amazon EC2. Há vários serviços de registro de domínio e de hospedagem DNS de terceiros disponíveis para isso, ou você pode usar o [Amazon Route 53](#).

## Etapa 1: habilitar o TLS no servidor

Este procedimento o auxilia no processo de configuração do TLS no Amazon Linux 2 com um certificado digital autoassinado.

### Note

Um certificado autoassinado é aceitável para testes, mas não para produção. Quando você expõe seu certificado autoassinado na Internet, os visitantes de seu site recebem avisos de segurança.

Para habilitar o TLS em um servidor

1. [Conecte-se à sua instância \(p. 11\)](#) e confirme se o Apache está em execução.

```
[ec2-user ~]$ sudo systemctl is-enabled httpd
```

Se o valor retornado não for "habilitado", inicie o Apache e configure-o para iniciar sempre que o sistema for inicializado.

```
[ec2-user ~]$ sudo systemctl start httpd && sudo systemctl enable httpd
```

2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. Esse processo pode levar alguns minutos, mas é importante ter certeza de que você tem as atualizações de segurança e correções de bug mais recentes.

### Note

A opção `-y` instala as atualizações sem solicitar confirmação. Para examinar as atualizações antes da instalação, você pode omitir essa opção.

```
[ec2-user ~]$ sudo yum update -y
```

3. Agora que sua instância está atualizada, adicione o suporte ao TLS instalando o módulo `mod_ssl` do Apache.

```
[ec2-user ~]$ sudo yum install -y mod_ssl
```

Sua instância agora possui os seguintes arquivos que você usará para configurar seu servidor seguro e criar um certificado para teste:

- `/etc/httpd/conf.d/ssl.conf`

O arquivo de configuração para `mod_ssl`. Contém as diretrizes que informam ao Apache onde encontrar chaves de criptografia e certificados, as versões do protocolo TLS a serem permitidas e as cifras de criptografia a serem aceitas.

- `/etc/pki/tls/certs/make-dummy-cert`

Um script para gerar um certificado X.509 autoassinado e uma chave privada para o seu host de servidor. Esse certificado é útil para testar se o Apache está configurado corretamente para usar o TLS. Como não oferece prova de identidade, ele não deve ser usado na produção. Caso contrário, avisos nos navegadores da Web serão exibidos.

4. Execute o script para gerar um certificado fictício autoassinado e uma chave para teste.

```
[ec2-user ~]$ cd /etc/pki/tls/certs  
sudo ./make-dummy-cert localhost.crt
```

Isso gera um novo arquivo `localhost.crt` no diretório `/etc/pki/tls/certs/`. O nome do arquivo especificado corresponde ao padrão atribuído na diretiva `SSLCertificateFile` em `/etc/httpd/conf.d/ssl.conf`.

Esse arquivo contém um certificado autoassinado e a chave privada do certificado. O Apache requer que o certificado e a chave estejam no formato PEM, que consiste em caracteres ASCII codificados em Base64 enquadados pelas linhas "BEGIN" e "END", como neste exemplo.

```
-----BEGIN PRIVATE KEY-----  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQD2KKx/8Zk94mlq  
3gQMZF9ZN66Ls19+3tHAgQ5Fpo9KJDhzLjOOC18u1PTcGmAah5kEitCEC0wzmNeo  
BC10wYR6G0rGaKtK9Dn7CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vr  
GvwnKoMh3D1K44D9dX7IDua2PlYx5+eroA+1Lqf32ZSaAO0bBIMIYTHigwbHMzOT  
...  
56tE7THvH7vOEf4/iUOsIrEzaMaJ0mqkmY1A70qQGQKBgBF3H1qNRNHuyMcPODFs  
27hDzPDinrqeuSEvoZIggkDMlh2irTiipJ/GhkvtPoQ1v0fK/Vxw8vSgeaBuhwJvS  
LXU9HvYq0U604FgD3nAyB9hI0BE13r1HjUvbjT7moH+RhnNz6eqqdscCS09VtRAo  
4Q0vAqOa8UheYeoxLdWcHaLP  
-----END PRIVATE KEY-----  
  
-----BEGIN CERTIFICATE-----  
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvCNQELBQAwgbExCzAJBgNVBAYTAi0t  
MRIwEAYDVQQIDAlTb21lU3RhGUxEТАPБgNVBAcMCFНvбWVДaXR5MRkwFwYDVQK  
DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWxv  
bml0MRkwFwYDVQQDDBBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvCNQkBFhVv  
...  
z5rRUE/XzxRLBZooWZpNWTXJkQ3uFYH6s/sBwtHpKKZMzOvDedREjNKAvk4ws6F0  
CuIjvubtUysVyQoMVPQ97ldeakHWeRMiEJFXg6kZZ0vrGvwnKoMh3D1K44D9d1U3  
WanXWehT6FiSzvB4sTEXXJN2jdw8g+sHGnZ8zCosclknYhRcVD2vnBlZJKSzvak  
3ZazhBxtQSukFMOnWPP2a0DMMFГYUH0d0BQE8sBJxg==  
-----END CERTIFICATE-----
```

Os nomes de arquivos e as extensões são uma conveniência e não têm efeito na função. Por exemplo, você pode chamar um certificado de `cert.crt`, `cert.pem` ou de um outro nome de arquivo qualquer, desde que a diretiva relacionada no arquivo `ssl.conf` use o mesmo nome.

**Note**

Ao substituir os arquivos TLS padrão por seus próprios arquivos personalizados, verifique se eles estão no formato PEM.

5. Abra o arquivo `/etc/httpd/conf.d/ssl.conf` usando seu editor de texto preferido (como o vim ou o nano) e comente a linha a seguir, porque o certificado fictício autoassinado também contém a chave. Se você não assinalar o comentário desta linha antes de concluir a próxima etapa, o serviço do Apache não conseguirá ser iniciado.

```
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

6. Reinicie o Apache.

```
[ec2-user ~]$ sudo systemctl restart httpd
```

**Note**

Verifique se a porta TCP 443 está acessível em sua instância do EC2, conforme descrito anteriormente.

7. Seu servidor da Web do Apache agora deve oferecer suporte a HTTPS (HTTP seguro) por meio da porta 443. Teste-o digitando o endereço IP ou o nome do domínio totalmente qualificado de sua instância do EC2 em uma barra de URL de um navegador com o prefixo **https://**.

Como você está se conectando a um site com um certificado de host autoassinado não confiável, o navegador poderá exibir uma série de avisos de segurança. Ignore os avisos e continue para o site.

Se a página de teste padrão do Apache for aberta, a configuração do TLS no servidor estará correta. Todos os dados que passam entre o navegador e o servidor agora estão criptografados.

**Note**

Para impedir que os visitantes do site encontrem telas de avisos, você precisa obter um certificado assinado por uma CA confiável que, além de criptografar, também autentique você publicamente como o proprietário do site.

## Etapa 2: obter um certificado assinado por uma CA

Você pode seguir este processo para obter um certificado assinado por uma CA:

- Gere uma solicitação de assinatura de certificado (CSR) a partir de uma chave privada
- Enviar a CSR para uma autoridade de certificação (CA)
- Obtenha um certificado de host assinado
- Configure o Apache para usá-lo

Um certificado de host TLS X.509 autoassinado é idêntico em termos criptológicos a um certificado assinado por uma CA. A diferença é social, não matemática. Uma CA promete validar, no mínimo, a propriedade de um domínio antes de emitir um certificado para um candidato. Cada navegador da Web contém uma lista de CAs confiáveis pelo fornecedor do navegador para fazer isso. Primariamente, um certificado X.509 consiste em uma chave pública, que corresponde à chave privada do servidor, e uma assinatura pela CA que é vinculada criptograficamente à chave pública. Quando um navegador se conecta

a um servidor da Web por meio de HTTPS, o servidor apresenta um certificado ao navegador para verificação em sua lista de CAs confiáveis. Se o assinante estiver na lista ou for acessível por meio de uma cadeia de confiança que consiste em outros assinantes confiáveis, o navegador negociará um canal rápido de dados criptografados com o servidor e carregará a página.

Geralmente, os certificados são caros devido ao trabalho envolvido na validação das solicitações, portanto, vale a pena comparar os preços. Algumas CAs oferecem certificados de nível básico gratuitamente. Entre essas CAs, a mais notável é o projeto [Let's Encrypt](#), que também oferece suporte à automação de criação de certificados e ao processo de renovação. Para obter mais informações sobre como usar a Let's Encrypt como sua CA, consulte [Automação de certificados: Let's Encrypt com o Certbot no Amazon Linux 2 \(p. 36\)](#).

Se você planeja oferecer serviços de nível comercial, o [AWS Certificate Manager](#) é uma boa opção.

É importante ter um certificado de host subjacente. Desde 2019, grupos [governamentais](#) e do [setor](#) recomendam usar um tamanho de chave (módulo) mínimo de 2.048 bits para chaves de RSA para a proteção de documentos até 2030. O tamanho do módulo padrão gerado pela OpenSSL no Amazon Linux 2 é de 2048 bits, que é adequada para ser usada em um certificado assinado por uma CA. No procedimento a seguir, uma etapa opcional é fornecida para aqueles que desejam uma chave personalizada, por exemplo, uma com módulo maior ou que usa um algoritmo diferente de criptografia.

As instruções para adquirir certificados de host assinados pela CA não funcionarão, a menos que você possua um domínio DNS registrado e hospedado.

#### Para obter um certificado assinado por uma CA

1. [Conecte-se à sua instância \(p. 11\)](#) e navegue até `/etc/pki/tls/private/`. Este é o diretório onde você armazenará a chave privada do servidor para TLS. Se você preferir usar uma chave de host existente para gerar a CSR, vá para a Etapa 3.
2. (Opcional) Gerar uma nova chave privada. Estes são alguns exemplos de configurações de chave. Qualquer uma das chaves resultantes funciona com seu servidor Web, mas elas variam no grau e no tipo de segurança que elas implementam.
  - Exemplo 1: criar uma chave host de RSA padrão. O arquivo resultante, `custom.key`, é uma chave privada de RSA de 2048 bits.

```
[ec2-user ~]$ sudo openssl genrsa -out custom.key
```

- Exemplo 2: criar uma chave de RSA mais forte com um módulo maior. O arquivo resultante, `custom.key`, é uma chave privada de RSA de 4096 bits.

```
[ec2-user ~]$ sudo openssl genrsa -out custom.key 4096
```

- Exemplo 3: criar uma chave de RSA de 4096 bits criptografada com proteção por senha. O arquivo resultante, `custom.key`, é uma chave privada de RSA de 4096 bits criptografada com a cifra AES-128.

#### Important

A criptografia da chave fornece maior segurança, mas como uma chave criptografada requer uma senha, os serviços que dependem dela não podem ser iniciados automaticamente. Sempre que usar essa chave, você precisará fornecer a senha (no exemplo anterior, "abcde12345") por meio de uma conexão SSH.

```
[ec2-user ~]$ sudo openssl genrsa -aes128 -passout pass:abcde12345 -out custom.key 4096
```

- Exemplo 4: criar uma chave usando uma cifra não RSA. A criptografia RSA pode ser relativamente devagar devido ao tamanho de suas chaves públicas, que são baseadas no produto de dois

números primos grandes. No entanto, é possível criar chaves para TLS que usam códigos não RSA. As chaves baseadas em matemática de curvas elípticas são menores e computacionalmente mais rápidas para fornecer um nível de segurança equivalente.

```
[ec2-user ~]$ sudo openssl ecparam -name prime256v1 -out custom.key -genkey
```

O resultado é uma chave privada de curva elíptica de 256 bits que usa prime256v1, uma "curva nomeada" compatível com OpenSSL. A força de criptografia é um pouco maior que uma chave de RSA de 2048 bits, [de acordo com o NIST](#).

#### Note

Nem todas as CAs fornecem o mesmo nível de suporte para chaves baseadas em curvas elípticas como para chaves de RSA.

Verifique se a nova chave privada tem a propriedade e permissões altamente restritivas (owner=root, group=root, leitura/gravação para o proprietário somente). O comando será o mostrado no exemplo a seguir.

```
[ec2-user ~]$ sudo chown root:root custom.key
[ec2-user ~]$ sudo chmod 600 custom.key
[ec2-user ~]$ ls -al custom.key
```

Os comandos anteriores produzem o resultado a seguir.

```
-rw----- root root custom.key
```

Depois de criar e configurar uma chave satisfatória, você pode criar uma CSR.

3. Crie uma CSR usando sua chave preferida. O exemplo a seguir usa **custom.key**.

```
[ec2-user ~]$ sudo openssl req -new -key custom.key -out csr.pem
```

A OpenSSL abre uma caixa de diálogo e solicita a informação exibida na tabela a seguir. Todos os campos, exceto Common Name (Nome comum), são opcionais para um certificado de host básico validado por domínio.

Nome	Descrição	Exemplo
Nome do país	A abreviação ISO de duas letras para seu país.	US (=Estados Unidos)
Nome do estado ou província	O nome do estado ou província onde sua organização está localizada. Este nome não pode ser abreviado.	Washington
Nome da localidade	A localização de sua organização, como uma cidade.	Seattle
Nome da organização	A razão social completa da sua organização. Não abrevie o nome de sua organização.	Corporação de exemplo
Nome da unidade organizacional	Informações organizacionais adicionais, se houver.	Departamento de exemplo

Nome	Descrição	Exemplo
Nome comum	Esse valor deve corresponder exatamente ao endereço Web que você espera que os usuários digitem em um navegador. Geralmente, isso significa um nome de domínio com um nome de host ou alias prefixados na forma <b>www.example.com</b> . Para teste com um certificado autoassinado e nenhuma resolução DNS, o nome comum pode consistir apenas no nome do host. As CAs também oferecem certificados mais caros que aceitam nomes curingas como <b>*.example.com</b> .	www.example.com
Endereço de e-mail	O endereço de e-mail do administrador do servidor.	someone@example.com

Finalmente, a OpenSSL solicita uma senha de desafio opcional. Essa senha se aplica somente à CSR e às transações entre você e sua CA, portanto, siga as recomendações da CA sobre este e o outro campo opcional, nome da empresa opcional. A senha de desafio da CSR não tem nenhum efeito sobre a operação do servidor.

O arquivo resultante **csr.pem** contém sua chave pública, a assinatura digital de sua chave pública e os metadados que você inseriu.

- Envie a CSR a uma CA. Geralmente, isso consiste em abrir seu arquivo de CSR em um editor de texto e copiar o conteúdo em um formulário da Web. Neste momento, pode ser solicitado que você forneça um ou mais nomes alternativos da entidade (SANs) para serem colocados no certificado. Se **www.example.com** for o nome comum, **example.com** seria um bom SAN e vice-versa. Um visitante de seu site que digitar qualquer um desses nomes verá uma conexão livre de erros. Se o formulário da Web de sua CA permitir, inclua o nome comum na lista de SANs. Algumas CAs o incluem automaticamente.

Depois que sua solicitação é aprovada, você recebe um novo certificado de host assinado pela CA. Você também pode receber uma instrução para fazer download de um arquivo de certificado intermediário que contém os certificados adicionais necessários para concluir a cadeia de confiança da CA.

#### Note

Sua CA pode enviar a você arquivos em vários formatos com várias finalidades. Para este tutorial, você deve usar apenas um arquivo de certificado em formato PEM, que geralmente (mas nem sempre) é identificado por uma extensão de arquivo **.pem** ou **.crt**. Se você não tiver certeza sobre qual arquivo usar, abra os arquivos com um editor de texto e localize um que contenha um ou mais blocos com a linha a seguir.

```
-----BEGIN CERTIFICATE-----
```

O arquivo também deve terminar com a linha a seguir.

```
-----END CERTIFICATE-----
```

Você também pode testar um arquivo na linha de comando da forma a seguir.

```
[ec2-user certs]$ openssl x509 -in certificate.crt -text
```

Verifique se as linhas aparecem no arquivo. Não use os arquivos que terminam com .p7b, .p7c ou extensões de arquivo semelhantes.

5. Coloque o novo certificado assinado pela CA e quaisquer certificados intermediários no diretório /etc/pki/tls/certs.

**Note**

Há várias maneiras para fazer upload do novo certificado para a instância do EC2, mas a maneira mais simples e informativa é abrir um editor de texto (vi, nano, bloco de notas etc.) no seu computador local e na sua instância e, em seguida, copiar e colar os conteúdos do arquivo entre eles. Você precisa de permissões raiz [sudo] ao realizar essas operações na instância do EC2. Dessa forma, você vê imediatamente se há algum problema de permissão ou de caminho. No entanto, tenha cuidado para não adicionar mais linhas ao copiar o conteúdo ou ao alterá-lo de alguma maneira.

No diretório /etc/pki/tls/certs, verifique se a propriedade do arquivo, o grupo e as configurações de permissão correspondem aos padrões altamente restritivos do Amazon Linux 2 (owner=root, group=root, leitura/gravação para o proprietário somente). O exemplo a seguir mostra os comandos a serem usados.

```
[ec2-user certs]$ sudo chown root:root custom.crt
[ec2-user certs]$ sudo chmod 600 custom.crt
[ec2-user certs]$ ls -al custom.crt
```

Esses comandos devem produzir o resultado a seguir.

```
-rw----- root root custom.crt
```

As permissões para o arquivo de certificado intermediário são menos estritas (owner=root, group=root, proprietário pode gravar, grupo pode ler, mundo pode ler). O exemplo a seguir mostra os comandos a serem usados.

```
[ec2-user certs]$ sudo chown root:root intermediate.crt
[ec2-user certs]$ sudo chmod 644 intermediate.crt
[ec2-user certs]$ ls -al intermediate.crt
```

Esses comandos devem produzir o resultado a seguir.

```
-rw-r--r-- root root intermediate.crt
```

6. Coloque a chave privada que você usou para criar o CSR no diretório /etc/pki/tls/private/.

**Note**

Há várias maneiras para fazer upload da chave personalizada para a instância do EC2, mas a maneira mais simples e informativa é abrir um editor de texto (vi, nano, bloco de notas etc.) no seu computador local e na sua instância e, em seguida, copiar e colar os conteúdos do arquivo entre eles. Você precisa de permissões raiz [sudo] ao realizar essas operações na instância do EC2. Dessa forma, você vê imediatamente se há algum problema de permissão ou de caminho. No entanto, tenha cuidado para não adicionar mais linhas ao copiar o conteúdo ou ao alterá-lo de alguma maneira.

No diretório /etc/pki/tls/private, use os comandos a seguir para verificar se a propriedade do arquivo, o grupo e as configurações de permissão correspondem aos padrões altamente restritivos do Amazon Linux 2 (owner=root, group=root, leitura/gravação para o proprietário somente).

```
[ec2-user private]$ sudo chown root:root custom.key
[ec2-user private]$ sudo chmod 600 custom.key
[ec2-user private]$ ls -al custom.key
```

Esses comandos devem produzir o resultado a seguir.

```
-rw----- root root custom.key
```

7. Edite `/etc/httpd/conf.d/ssl.conf` para refletir seu novo certificado e arquivos de chave.
  - a. Forneça o caminho e o nome do arquivo do certificado de host assinado por CA na diretiva `SSLCertificateFile` do Apache:

```
SSLCertificateFile /etc/pki/tls/certs/custom.crt
```
  - b. Se você receber um arquivo de certificado intermediário (`intermediate.crt` neste exemplo), forneça o caminho e o nome do arquivo usando a diretiva `SSLCACertificateFile` do Apache:

```
SSLCACertificateFile /etc/pki/tls/certs/intermediate.crt
```

#### Note

Algumas CAs combinam os certificados de host e os certificados intermediários em um único arquivo, o que torna a diretiva `SSLCACertificateFile` desnecessária. Consulte as instruções fornecidas pela CA.

- c. Forneça o caminho e o nome do arquivo da chave privada (`custom.key` neste exemplo) na diretiva `SSLCertificateKeyFile` do Apache:

```
SSLCertificateKeyFile /etc/pki/tls/private/custom.key
```

8. Salve o `/etc/httpd/conf.d/ssl.conf` e reinicie o Apache.

```
[ec2-user ~]$ sudo systemctl restart httpd
```

9. Teste seu servidor inserindo seu nome de domínio em uma barra de URL do navegador com o prefixo `https://`. Seu navegador deve carregar a página de teste via HTTPS sem gerar erros.

## Etapa 3: testar e intensificar a configuração de segurança

Depois que o SSL/TLS estiver operacional e exposto ao público, você precisará testar se ele é realmente seguro. É fácil fazer isso usando serviços online, como o [Qualys SSL Labs](#) que executa uma análise completa e gratuita de sua configuração de segurança. Com base nos resultados, você pode decidir intensificar a configuração de segurança padrão controlando quais protocolos você aceita, quais cifras você prefere e quais você exclui. Para obter mais informações, consulte [como a Qualys formula suas pontuações](#).

#### Important

Os testes no mundo real são cruciais para a segurança do servidor. Pequenos erros de configuração podem resultar em rupturas de segurança sérias e em perda de dados. Como as práticas de segurança recomendadas são alteradas constantemente em resposta a pesquisas e a ameaças emergentes, auditorias periódicas da segurança são essenciais para uma boa administração do servidor.

No site [Qualys SSL Labs](#), digite o nome do domínio totalmente qualificado de seu servidor no formato **www.example.com**. Depois de dois minutos, você recebe uma classificação (de A a F) para seu site e um detalhamento dos resultados. A tabela a seguir resume o relatório de um domínio com configurações idênticas à configuração padrão do Apache no Amazon Linux 2 e um certificado padrão do Certbot.

Classificação geral	B
Certificado	100%
Suporte ao protocolo	95%
Troca de chaves	70%
Intensidade da cifra	90%

Embora a visão geral mostre que a configuração é mais sólida, o relatório detalhado sinaliza vários possíveis problemas, listados aqui em ordem de gravidade:

- ✗ A codificação RC4 é compatível com o uso por determinados navegadores mais antigos. Uma cifra é o núcleo matemático de um algoritmo de criptografia. A RC4, uma cifra rápida usada para criptografar fluxos de dados TLS, é conhecida por ter várias [fraquezas sérias](#). A menos que você tenha boas razões para oferecer suporte a navegadores legados, você deve desabilitar isso.
- ✗ Versões antigas do TLS são compatíveis. A configuração é compatível com o TLS 1.0 (já obsoleto) e o TLS 1.1 (em um caminho para a reprovação). Apenas o TLS 1.2 é recomendado desde 2018.
- ✗ O sigilo de encaminhamento não é totalmente compatível. O [sigilo encaminhado](#) é um recurso de algoritmos que criptografam usando chaves de sessão temporárias (efêmeras) derivadas da chave privada. Na prática, isso significa que os atacantes não podem descriptografar dados HTTPS mesmo que tenham a chave privada de longo prazo de um servidor Web.

Para corrigir e preparar futuramente a configuração do TLS

1. Abra o arquivo de configuração `/etc/httpd/conf.d/ssl.conf` em um editor de texto e comente as seguintes linhas digitando “#” no início delas.

```
#SSLProtocol all -SSLv3
```

2. Adicione a seguinte diretiva:

```
#SSLProtocol all -SSLv3
SSLProtocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
```

Essa diretiva desabilita explicitamente as versões 2 e 3 do SSL, bem como as versões 1.0 e 1.1 do TLS. O servidor agora se recusa a aceitar conexões criptografadas com clientes que não estejam usando o TLS 1.2. A expressão detalhada na diretriz transmite mais claramente, para um leitor humano, para que o servidor está configurado.

#### Note

Desabilitar as versões 1.0 e 1.1 do TLS dessa forma bloqueia o acesso ao seu site de uma pequena porcentagem de navegadores da Web desatualizados.

Para modificar a lista de cifras permitidas

1. No arquivo de configuração `/etc/httpd/conf.d/ssl.conf`, localize a seção com a diretiva `SSLCipherSuite` e comente a linha existente ao inserir “#” no início dela.

```
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5
```

2. Especifique conjuntos de criptografia explícitos e uma ordem de cifra que priorize o sigilo antecipado e evite cifras inseguras. A diretiva `SSLCipherSuite` usada aqui é baseada na saída do [gerador de configuração SSL do Mozilla](#), que adapta uma configuração TLS ao software específico em execução no seu servidor. (Para mais informações, consulte o recurso útil do Mozilla [segurança/TLS do lado do servidor](#).) Primeiro, determine suas versões do Apache e do OpenSSL usando os comandos a seguir.

```
[ec2-user ~]$ yum list installed | grep httpd  
[ec2-user ~]$ yum list installed | grep openssl
```

Por exemplo, se a informação exibida for Apache 2.4.34 e OpenSSL 1.0.2, insira esses valores no gerador. Se você escolher o modelo de compatibilidade "moderno", isso criará uma diretiva `SSLCipherSuite` que impõe a segurança de forma agressiva, mas ainda funciona para a maioria dos navegadores. Se o software não oferecer suporte à configuração moderna, você poderá atualizá-lo ou escolher a configuração "intermediária".

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-  
CHACHA20-POLY1305:  
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:  
ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-  
AES128-SHA256
```

As cifras selecionadas têm ECDHE em seus nomes, o que significa Elliptic Curve Diffie-Hellman Ephemeral (Curva elíptica de Diffie-Hellman efêmera). O termo ephemeral (efêmera) indica forward secrecy. Como subproduto, essas cifras não são compatíveis com RC4.

Recomendamos que você use uma lista explícita de cifras em vez de confiar em padrões ou em diretrizes concisas cujo conteúdo não é visível.

Copie a diretiva gerada em `/etc/httpd/conf.d/ssl.conf`.

#### Note

Embora sejam mostradas em várias linhas aqui para facilitar a leitura, a diretriz deve estar em uma única linha quando copiada para `/etc/httpd/conf.d/ssl.conf` com apenas dois pontos (sem espaços) entre os nomes das cifras.

3. Por fim, remova o comentário da linha a seguir, excluindo o "#" no início dela.

```
#SSLHonorCipherOrder on
```

Essa diretiva força o servidor a preferir cifras de alta classificação incluindo (neste caso) aquelas que oferecem suporte a forward secrecy. Com essa diretiva ativada, o servidor tenta estabelecer uma conexão altamente segura antes de voltar a usar cifras permitidas com menos segurança.

Depois de concluir esses dois procedimentos, salve as alterações em `/etc/httpd/conf.d/ssl.conf` e reinicie o Apache.

Se você testar o domínio novamente no [Qualys SSL Labs](#), você verá que a vulnerabilidade do RC4 e outros avisos desapareceram e o resumo se parece ao exemplo a seguir.

Classificação geral	A
Certificado	100%

Suporte ao protocolo	100%
Troca de chaves	90%
Intensidade da cifra	90%

Cada atualização do OpenSSL apresenta novas cifras e retira o suporte às cifras antigas. Mantenha sua instância do EC2 do Amazon Linux 2 atualizada e fique atento às notificações de segurança da [OpenSSL](#) e às notícias sobre novas descobertas em segurança na imprensa técnica.

## Troubleshoot

- Meu servidor da Web do Apache não inicia, a menos que eu digite uma senha

Esse é comportamento esperado se você tiver instalado uma chave privada de servidor criptografada e protegida por senha.

Você pode remover a criptografia e a solicitação de senha da chave. Supondo que você tenha uma chave de RSA privada criptografada chamada `custom.key` no diretório padrão, e que a senha seja `abcde12345`, execute os comandos a seguir na sua instância do EC2 para gerar uma versão descriptografada da chave:

```
[ec2-user ~]$ cd /etc/pki/tls/private/  
[ec2-user private]$ sudo cp custom.key custom.key.bak  
[ec2-user private]$ sudo openssl rsa -in custom.key -passin pass:abcde12345 -out  
    custom.key.nocrypt  
[ec2-user private]$ sudo mv custom.key.nocrypt custom.key  
[ec2-user private]$ sudo chown root:root custom.key  
[ec2-user private]$ sudo chmod 600 custom.key  
[ec2-user private]$ sudo systemctl restart httpd
```

O Apache agora deve iniciar sem solicitar uma senha a você.

- Obtenho erros ao executar `sudo yum install -y mod_ssl`.

Quando estiver instalando os pacotes necessários para SSL, você verá erros como os exibidos a seguir.

```
Error: httpd24-tools conflicts with httpd-tools-2.2.34-1.16.amzn1.x86_64  
Error: httpd24 conflicts with httpd-2.2.34-1.16.amzn1.x86_64
```

Geralmente, isso significa que sua instância do EC2 não está executando o Amazon Linux 2. Este tutorial comporta somente instâncias recentemente criadas em uma AMI oficial do Amazon Linux 2.

## Automação de certificados: Let's Encrypt com o Certbot no Amazon Linux 2

A autoridade de certificado [Let's Encrypt](#) é a peça central de um esforço da Electronic Frontier Foundation (EFF) para criptografar toda a Internet. Em linha com esse objetivo, os certificados de host da Let's Encrypt são projetados para serem criados, validados, instalados e mantidos com intervenção humana mínima. Os aspectos automatizados do gerenciamento de certificados são realizados por um agente de software em execução no seu servidor Web. Depois que você instala e configura o agente, ele se comunica de forma segura com a Let's Encrypt e executa tarefas administrativas no Apache e no sistema de gerenciamento de chaves. Este tutorial usa o agente gratuito da [Certbot](#) porque ele permite que você forneça uma chave de criptografia personalizada como a base para seus certificados ou que o próprio agente crie uma chave

com base em seus padrões. Você também pode configurar o Certbot para renovar seus certificados regularmente sem interação humana, conforme descrito abaixo em [Para automatizar o Certbot \(p. 40\)](#). Para obter mais informações, consulte o [Guia do usuário](#) e as [páginas do manual](#) do Certbot.

O Certbot não é oficialmente compatível com o Amazon Linux 2, mas está disponível para download e funciona corretamente depois de instalado. Recomendamos que você faça os seguintes backups para proteger seus dados e evitar inconveniência:

- Antes de começar, faça um snapshot do seu volume raiz do Amazon EBS. Isso permite que você restaure o estado original de sua instância do EC2. Para obter informações sobre como criar snapshots do EBS, consulte [Criar snapshots de Amazon EBS \(p. 1307\)](#).
- O procedimento abaixo requer que você edite seu arquivo `httpd.conf`, que gerencia a operação do Apache. O Certbot faz suas próprias alterações automatizadas nesse e em outros arquivos de configuração. Faça uma cópia de backup de seu diretório `/etc/httpd` inteiro caso você precise restaurá-lo.

## Preparar-se para instalar

Execute os seguintes procedimentos antes de instalar o Certbot.

1. Faça download dos pacotes do repositório Extra Packages for Enterprise Linux (EPEL) 7. Eles são necessários para fornecer as dependências necessárias pelo Certbot.
  - a. Navegue até o diretório do início (`/home/ec2-user`). Faça download do EPEL com o comando a seguir.

```
[ec2-user ~]$ sudo wget -r --no-parent -A 'epel-release*.rpm' https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/
```

- b. Instale os pacotes do repositório conforme exibido no comando a seguir.

```
[ec2-user ~]$ sudo rpm -Uvh dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release*.rpm
```

- c. Habilite o EPEL conforme exibido no comando a seguir.

```
[ec2-user ~]$ sudo yum-config-manager --enable epel*
```

Você pode confirmar que o EPEL está habilitado com o comando a seguir.

```
[ec2-user ~]$ sudo yum repolist all
```

Esse comando deve retornar informações semelhante às exibidas a seguir.

```
[ec2-user ~]$  
...  
epel/x86_64                               Extra Packages for Enterprise Linux 7 - x86_64  
                                         enabled: 12949+175  
epel-debuginfo/x86_64                      Extra Packages for Enterprise Linux 7 - x86_64  
  - Debug                                     enabled:      2890  
epel-source/x86_64                         Extra Packages for Enterprise Linux 7 - x86_64  
  - Source                                    enabled:        0  
epel-testing/x86_64                        Extra Packages for Enterprise Linux 7 -  
  Testing - x86_64                           enabled:    778+12  
epel-testing-debuginfo/x86_64                Extra Packages for Enterprise Linux 7 -  
  Testing - x86_64 - Debug                   enabled:      107
```

```
epel-testing-source/x86_64           Extra Packages for Enterprise Linux 7 -  
Testing - x86_64 - Source            enabled: 0  
...  
...
```

2. Edite o arquivo de configuração do Apache, /etc/httpd/conf/httpd.conf. Localize a diretiva "Listen 80" e adicione as seguintes linhas após ela, substituindo os nomes de domínio de exemplo pelo nome comum real e pelo nome de assunto alternativo (SAN).

```
<VirtualHost *:80>  
    DocumentRoot "/var/www/html"  
    ServerName "example.com"  
    ServerAlias "www.example.com"  
</VirtualHost>
```

Salve o arquivo e reinicie o Apache.

```
[ec2-user ~]$ sudo systemctl restart httpd
```

## Instalar e executar o Certbot

Este procedimento é baseado na documentação do EFF para instalar o Certbot no [Fedora](#) e no [RHEL 7](#). Ele descreve o uso padrão do Certbot, resultando em um certificado baseado em uma chave RSA de 2048 bits.

1. Instale pacotes e dependências do Certbot usando o comando a seguir.

```
[ec2-user ~]$ sudo yum install -y certbot python2-certbot-apache
```

2. Execute o Certbot.

```
[ec2-user ~]$ sudo certbot
```

3. No prompt "Digite o endereço de e-mail (usado para avisos urgentes de renovação e segurança)", digite um endereço de contato e pressione Enter.
4. Concorde com os Termos de serviço do Let's Encrypt no prompt. Digite "A" e pressione Enter para continuar.

```
- - - - -  
Please read the Terms of Service at  
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must  
agree in order to register with the ACME server at  
https://acme-v02.api.letsencrypt.org/directory  
- - - - -  
(A)gree/(C)ancel: A
```

5. Para colocar você na lista de correspondência na autorização para o EFF, digite "S" ou "N" e pressione Enter.
6. O Certbot exibe o nome comum e o nome de assunto alternativo (SAN) que você forneceu no bloco VirtualHost.

```
Which names would you like to activate HTTPS for?  
- - - - -  
1: example.com  
2: www.example.com  
- - - - -  
Select the appropriate numbers separated by commas and/or spaces, or leave input
```

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Automação de certificados: Let's Encrypt  
com o Certbot no Amazon Linux 2

blank to select all options shown (Enter 'c' to cancel):

Deixe a entrada em branco e pressione Enter.

7. O Certbot exibe a saída a seguir ao criar certificados e configurar o Apache. Em seguida, ele informa sobre o redirecionamento de consultas HTTP para HTTPS.

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for example.com
http-01 challenge for www.example.com
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/httpd/conf/httpd-le-ssl.conf
Deploying Certificate for example.com to VirtualHost /etc/httpd/conf/httpd-le-ssl.conf
Enabling site /etc/httpd/conf/httpd-le-ssl.conf by adding Include to root configuration
Deploying Certificate for www.example.com to VirtualHost /etc/httpd/conf/httpd-le-ssl.conf

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
- - - - -
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
- - - - -
Select the appropriate number [1-2] then [enter] (press 'c' to cancel):
```

Para permitir que os visitantes se conectem ao seu servidor por HTTP não criptografado, digite "1". Se você deseja aceitar somente conexões criptografadas via HTTPS, digite "2". Pressione Enter para enviar sua escolha.

8. O Certbot conclui a configuração do Apache e relata o êxito e outras informações.

```
Congratulations! You have successfully enabled https://example.com and
https://www.example.com

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=example.com
https://www.ssllabs.com/ssltest/analyze.html?d=www.example.com
- - - - -

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/certbot.oneeyedman.net/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/certbot.oneeyedman.net/privkey.pem
  Your cert will expire on 2019-08-01. To obtain a new or tweaked
  version of this certificate in the future, simply run certbot again
  with the "certonly" option. To non-interactively renew *all* of
  your certificates, run "certbot renew"
- Your account credentials have been saved in your Certbot
  configuration directory at /etc/letsencrypt. You should make a
  secure backup of this folder now. This configuration directory will
  also contain certificates and private keys obtained by Certbot so
  making regular backups of this folder is ideal.
```

9. Depois de concluir a instalação, teste e otimize a segurança do servidor, conforme descrito em [Etapa 3: testar e intensificar a configuração de segurança \(p. 33\)](#).

## Configurar a renovação automatizada de certificado

O Certbot é projetado para se tornar uma parte invisível resistente a erros do sistema de servidor. Por padrão, ele gera certificados de host com um tempo de expiração curto de 90 dias. Se você não tiver configurado o sistema para chamar o comando automaticamente, execute de novo o comando certbot manualmente antes da expiração. Este procedimento mostra como automatizar o Certbot configurando um trabalho cron.

Para automatizar o Certbot

1. Abra o arquivo /etc/crontab em um editor de texto, como vim ou nano, usando sudo. Como alternativa, use sudo crontab -e.
2. Adicione uma linha semelhante à seguinte e salve o arquivo.

```
39      1,13    *      *      *      root    certbot renew --no-self-upgrade
```

Esta é uma explicação de cada componente:

```
39 1,13 * * *
```

Programa a execução de um comando à 1h39 e às 13h39 todos os dias. Os valores selecionados são arbitrários, mas os desenvolvedores do Certbot sugerem executar o comando pelo menos duas vezes por dia. Isso garante que qualquer certificado comprometido seja revogado e substituído imediatamente.

```
root
```

O comando é executado com permissões root.

```
certbot renew --no-self-upgrade
```

O comando a ser executado. O subcomando renew faz com que o Certbot verifique todos os certificados obtidos anteriormente e renove aqueles que estão se aproximando da expiração. O sinalizador --no-self-upgrade impede que o Certbot se atualize sem sua intervenção.

3. Reinicie o daemon cron.

```
[ec2-user ~]$ sudo systemctl restart crond
```

## Tutorial: Hospedar um blog do WordPress no Amazon Linux 2

Os procedimentos a seguir ajudarão você a instalar, configurar e proteger um blog do WordPress na sua instância do Amazon Linux. Este tutorial é uma boa introdução para usar o Amazon EC2 no qual você tem controle total sobre um servidor web que hospeda seu blog do WordPress, o que não é típico com um serviço de hospedagem tradicional.

Você é responsável por atualizar os pacotes de software e manter os patches de segurança para seu servidor. Para uma instalação mais automatizada do WordPress que não exige interação direta com a configuração do servidor web, o AWS CloudFormation fornecerá um modelo do WordPress que também pode ajudá-lo a começar rapidamente. Para obter mais informações, consulte [Get started](#) (Comece a usar) no AWS CloudFormation User Guide (Guia do usuário do AWS CloudFormation). Se você preferir hospedar o blog do WordPress em uma instância do Windows, consulte [Implantar um blog do WordPress na instância do Windows do Amazon EC2](#) no Guia do usuário do Amazon EC2 para instâncias do Windows. Se precisar de uma solução de alta disponibilidade com um banco de dados desacoplado,

consulte [Deploying a high-availability WordPress website](#) (Implantar um site do WordPress de alta disponibilidade) no AWS Elastic Beanstalk Developer Guide (Guia do desenvolvedor do AWS Elastic Beanstalk).

**Important**

Esses procedimentos são destinados ao Amazon Linux. Para obter mais informações sobre outras distribuições, consulte a documentação específica. Muitas etapas deste tutorial não funcionam em instâncias Ubuntu. Para ajuda na instalação do WordPress em uma instância Ubuntu, consulte [WordPress](#) na documentação do Ubuntu.

Opção: concluir este tutorial usando a automação

Para concluir este tutorial usando a automação do AWS Systems Manager em vez das tarefas a seguir, execute um dos seguintes documentos de automação: [AWS Docs - Hosting A WordPress Blog - AL](#) (Amazon Linux) ou [AWS Docs - Hosting A WordPress Blog - AL2](#) (Amazon Linux 2).

Tópicos

- [Prerequisites \(p. 41\)](#)
- [Instalar o WordPress \(p. 41\)](#)
- [Próximas etapas \(p. 48\)](#)
- [Ajuda! Meu nome DNS público mudou e agora meu blog não está funcionando \(p. 49\)](#)

## Prerequisites

Este tutorial pressupõe que você tenha executado uma instância do Amazon Linux com um servidor web funcional que oferece suporte a PHP e banco de dados (MySQL ou MariaDB) seguindo todas as etapas em [Tutorial: Instalar um servidor web LAMP no Amazon Linux AMI \(p. 50\)](#) para a AMI do Amazon Linux ou [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 15\)](#) para o Amazon Linux 2. Este tutorial tem também etapas para configurar um security group para permitir tráfego de HTTP e HTTPS, bem como várias etapas para garantir que as permissões de arquivos sejam definidas corretamente para seu servidor web. Para obter informações sobre como adicionar regras ao seu security group, consulte [Adicionar regras a um grupo de segurança \(p. 1233\)](#).

Recomendamos veementemente que você associe um endereço IP elástico (EIP) à instância que está usando para hospedar um blog do WordPress. Isso impede que o endereço DNS público da sua instância mude e quebre sua instalação. Se você tiver um nome de domínio e quiser usá-lo para o blog, pode atualizar o registro DNS do nome de domínio para indicar ao seu endereço EIP (para obter ajuda com isso, contate seu provedor de nome de domínio). Você pode ter um endereço EIP associado a uma instância em execução, gratuitamente. Para obter mais informações, consulte [Endereços IP elásticos \(p. 975\)](#).

Se você ainda não tiver um nome de domínio para seu blog, pode registrar um nome de domínio com o Route 53 e associar o endereço EIP de sua instância com seu nome de domínio. Para obter mais informações, consulte [Registrar nomes de domínio usando o Amazon Route 53](#) no Guia do desenvolvedor do Amazon Route 53.

## Instalar o WordPress

Conecte-se à sua instância e baixe o pacote instalação do WordPress.

Para fazer download e descompactar o pacote instalação do WordPress

1. Faça download do pacote de instalação mais recente do WordPress com o comando wget. O comando a seguir deve baixar a versão mais recente.

```
[ec2-user ~]$ wget https://wordpress.org/latest.tar.gz
```

2. Descompacte e desarquive o pacote de instalação. A pasta de instalação é descompactada para uma pasta chamada `wordpress`.

```
[ec2-user ~]$ tar -xzf latest.tar.gz
```

Para criar um usuário de banco de dados e um banco de dados para a instalação do WordPress

Sua instalação do WordPress precisa armazenar informações, como publicações de blog e comentários de usuários, em um banco de dados. Esse procedimento ajuda você a criar um banco de dados para seu blog e um usuário autorizado a ler e salvar as informações.

1. Inicie o servidor do banco de dados.

- Amazon Linux 2

```
[ec2-user ~]$ sudo systemctl start mariadb
```

- AMI do Amazon Linux

```
[ec2-user ~]$ sudo service mysqld start
```

2. Faça login no servidor do banco de dados como usuário `root`. Insira a senha de `root` do banco de dados quando solicitado; ela poderá ser diferente da sua senha do sistema de `root` ou poderá até estar vazia, se você não tiver protegido seu servidor do banco de dados.

Se ainda não tiver protegido seu servidor do banco de dados, é muito importante que você faça isso. Para obter mais informações, consulte [Para proteger o servidor MariaDB \(p. 20\)](#) (Amazon Linux 2) ou [Para proteger o servidor do banco de dados \(p. 55\)](#) (AMI Amazon Linux).

```
[ec2-user ~]$ mysql -u root -p
```

3. Crie um usuário e uma senha para seu banco de dados do MySQL. Sua instalação do WordPress usa esses valores para se comunicar com seu banco de dados do MySQL. Digite o comando a seguir, substituindo um nome de usuário e uma senha exclusivos.

```
CREATE USER 'wordpress-user'@'localhost' IDENTIFIED BY 'your_strong_password';
```

Crie uma senha forte para seu usuário. Não use o caractere de aspa única (') na sua senha, pois isso quebrará o comando anterior. Para obter mais informações sobre como criar uma senha segura, visite <http://www.pctools.com/guides/password/>. Não reutilize uma senha existente e armazene essa senha em um lugar seguro.

4. Crie seu banco de dados. Dê ao seu banco de dados um nome descritivo e significativo, como `wordpress-db`.

#### Note

As marcas de pontuação que cercam o nome do banco de dados no comando abaixo são chamados backticks. A chave de backtick (^) costuma estar localizada acima da chave Tab de um teclado padrão. Backticks nem sempre são necessários, mas permitem que você use caracteres de outra forma ilegais, como hífens, no nome dos bancos de dados.

```
CREATE DATABASE `wordpress-db`;
```

5. Conceda privilégios completos para seu banco de dados ao usuário do WordPress criado anteriormente.

```
GRANT ALL PRIVILEGES ON `wordpress-db`.* TO "wordpress-user"@"localhost";
```

6. Limpe os privilégios do banco de dados para receber todas as suas alterações.

```
FLUSH PRIVILEGES;
```

7. Saia do cliente mysql.

```
exit
```

Para criar e editar o arquivo wp-config.php

A pasta de instalação do WordPress contém um arquivo de configuração de exemplo chamado `wp-config-sample.php`. Nesse procedimento, você copia esse arquivo e o edita para caber na sua configuração específica.

1. Copie o arquivo `wp-config-sample.php` para um arquivo chamado `wp-config.php`. Isso cria um novo arquivo de configuração e mantém o arquivo de exemplo intacto como um backup.

```
[ec2-user ~]$ cp wordpress/wp-config-sample.php wordpress/wp-config.php
```

2. Edite o arquivo `wp-config.php` com seu editor de texto favorito (como o nano ou o vim) e insira os valores da instalação. Se você não tiver um editor de texto favorito, o nano é ideal para iniciantes.

```
[ec2-user ~]$ nano wordpress/wp-config.php
```

- a. Encontre a linha que define `DB_NAME` e altere `database_name_here` para o nome do banco de dados criado em [Step 4 \(p. 42\)](#) de [Para criar um usuário de banco de dados e um banco de dados para a instalação do WordPress \(p. 42\)](#).

```
define('DB_NAME', 'wordpress-db');
```

- b. Encontre a linha que define `DB_USER` e altere `username_here` para o usuário do banco de dados que você criou [Step 3 \(p. 42\)](#) de [Para criar um usuário de banco de dados e um banco de dados para a instalação do WordPress \(p. 42\)](#).

```
define('DB_USER', 'wordpress-user');
```

- c. Encontre a linha que define `DB_PASSWORD` e altere `password_here` para a senha mais forte que você criou em [Step 3 \(p. 42\)](#) de [Para criar um usuário de banco de dados e um banco de dados para a instalação do WordPress \(p. 42\)](#).

```
define('DB_PASSWORD', 'your_strong_password');
```

- d. Encontre a seção chamada `Authentication Unique Keys and Salts`. Esses valores `KEY` e `SALT` fornecem uma camada de criptografia para os cookies do navegador que os usuários do WordPress armazenam em suas máquinas locais. Basicamente, adicionar valores longos e aleatórios aqui deixa seu site mais seguro. Visite <https://api.wordpress.org/secret-key/1.1/salt/> para gerar aleatoriamente um conjunto de valores-chave que você pode copiar e colar no seu arquivo `wp-config.php`. Para colar texto em um terminal do PuTTY, coloque o cursor onde deseja colar texto e clique com o botão direito do mouse dentro do terminal do PuTTY.

Para obter mais informações sobre as chaves de segurança, acesse <https://wordpress.org/support/article/editing-wp-config-php/#security-keys>.

#### Note

Os valores abaixo são somente para fins de exemplo; não use esses valores para a instalação.

```
define('AUTH_KEY',         ' #U$$+[RXN8:b^-I_0(WU+_c+WFkI-c]o]-bHw+/'
Aj[wTwSiz<Qb[mghEXcRh-');
define('SECURE_AUTH_KEY',   'zsz._P=l/|y.Lq)XjlkW5y5NJ76E6EJ.AV0pCKZZB,*-*r ?6OP
$eJT@;+(ndIg');
define('LOGGED_IN_KEY',     'ju}qwre3V*+8f_zOWF?{LlGsQ]Ye@2Jh^,8x>)Y |;(^[Iw]Pi
+LG#A4R?7N`YB3');
define('NONCE_KEY',         'P(g62HeZxEes/lnI^i=H,[XwK9I&[2s|:?ON}VJM%?;v2v]v+;
+^9eXUahg@: :Cj');
define('AUTH_SALT',          'C$DpB4Hj[JK:{ql`sRVA:{:7yShy(9A@5wg+`JJVb1fk%-
Bx*M4(qc[Og%JT!h');
define('SECURE_AUTH_SALT',   'd!uRu#}+q#{f$Z?Z9uFPG.$.{+S{n~1M&%@-gL>U>NV<zpD-@2-
Es7Q1O-bp28EKv');
define('LOGGED_IN_SALT',     ' ;j{00P*owzf)kVD+FVLn-- >. |Y%Ug4#I^*LVd9QeZ^&XmK/e(76mic
+&W&+^OP/');
define('NONCE_SALT',         '-97r*V/cgxLmp?Zy4zUU4r99QO_rGs2LTd%P; |
_e1tS)8_B/, .6[=UK<J_y9?JWG');
```

- e. Salve o arquivo e saia do seu editor de texto.

Para instalar seus arquivos do WordPress no documento-raiz do Apache

- Agora que você descompactou a pasta de instalação, criou um banco de dados e um usuário do MySQL e personalizou o arquivo de configuração do WordPress, está pronto para copiar seus arquivos de instalação à raiz do documento do servidor web para que possa executar o script de instalação que encerrará sua instalação. O local desses arquivos depende de se você quer que seu blog do WordPress esteja disponível na raiz real do seu servidor web (por exemplo, [my.public.dns.amazonaws.com](http://my.public.dns.amazonaws.com)) ou em um subdiretório ou em uma pasta sob a raiz (por exemplo, [my.public.dns.amazonaws.com/blog](http://my.public.dns.amazonaws.com/blog)).
- Se você quiser que o WordPress seja executado na raiz de documentos, copie o conteúdo do diretório de instalação do WordPress (mas não o diretório em si) da seguinte maneira:

```
[ec2-user ~]$ cp -r wordpress/* /var/www/html/
```

- Se você quiser que o WordPress seja executado em um diretório alternativo na raiz de documentos, crie primeiro esse diretório e, em seguida, copie os arquivos para ele. Neste exemplo, o WordPress será executado pelo diretório blog:

```
[ec2-user ~]$ mkdir /var/www/html/blog
[ec2-user ~]$ cp -r wordpress/* /var/www/html/blog/
```

#### Important

Para fins de segurança, se você não estiver seguro para o procedimento seguinte imediatamente, pare o Apache Web Server (`httpd`) agora. Depois de mover sua instalação para a raiz de documentos do Apache, o script de instalação do WordPress estará desprotegido e um invasor poderia ganhar acesso ao seu blog se o Apache Web Server estiver sendo executado. Para interromper o servidor web Apache, insira o comando `sudo service httpd stop`. Se você estiver passando para o procedimento seguinte, não precisa parar o Apache Web Server.

Para permitir que o WordPress use permalinks

Os permalinks do WordPress precisam usar arquivos .htaccess do Apache para funcionarem corretamente, mas isso não fica habilitado por padrão no Amazon Linux. Use o procedimento a seguir para permitir todas as substituições na raiz de documentos do Apache.

1. Abra o arquivo httpd.conf com seu editor de texto de preferência (como nano ou vim). Se você não tiver um editor de texto favorito, o nano é ideal para iniciantes.

```
[ec2-user ~]$ sudo vim /etc/httpd/conf/httpd.conf
```

2. Encontre a seção que começa com <Directory "/var/www/html">.

```
<Directory "/var/www/html">
#
# Possible values for the Options directive are "None", "All",
# or any combination of:
#   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
# The Options directive is both complicated and important. Please see
# http://httpd.apache.org/docs/2.4/mod/core.html#options
# for more information.
#
Options Indexes FollowSymLinks

#
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
AllowOverride None

#
# Controls who can get stuff from this server.
#
Require all granted
</Directory>
```

3. Altere a linha AllowOverride None na seção acima para AllowOverride All.

Note

Há múltiplas linhas AllowOverride nesse arquivo; altere a linha na seção <Directory "/var/www/html">.

```
AllowOverride All
```

4. Salve o arquivo e saia do seu editor de texto.

## Como instalar a biblioteca de desenhos gráficos PHP no Amazon Linux 2

A biblioteca de desenhos gráficos para PHP permite modificar imagens. Instale esta biblioteca caso você precise cortar a imagem do cabeçalho do blog. A versão do phpMyAdmin que você instalar poderá exigir uma versão mínima específica desta biblioteca (por exemplo, versão 7.2).

Use o comando a seguir para instalar a biblioteca de desenhos gráficos PHP no Amazon Linux 2. Por exemplo, se você instalou php7.2 da amazon-linux-extras como parte da instalação da pilha LAMP, este comando instalará a versão 7.2 da biblioteca de desenhos gráficos PHP.

```
[ec2-user ~]$ sudo yum install php-gd
```

Para verificar a versão instalada, use o seguinte comando:

```
[ec2-user ~]$ sudo yum list installed | grep php-gd
```

A seguir está um exemplo de saída:

php-gd.x86_64	7.2.30-1.amzn2	@amzn2extra-php7.2
---------------	----------------	--------------------

Para instalar a biblioteca de desenhos gráficos PHP no Amazon Linux AMI

A biblioteca de desenhos gráficos para PHP permite modificar imagens. Instale esta biblioteca caso você precise cortar a imagem do cabeçalho do blog. A versão do phpMyAdmin que você instalar poderá exigir uma versão mínima específica desta biblioteca (por exemplo, versão 7.2).

Para verificar quais versões estão disponíveis, use o seguinte comando:

```
[ec2-user ~]$ yum list | grep php-gd
```

Veja a seguir uma linha de exemplo da saída para a biblioteca de desenhos gráficos PHP (versão 7.2):

php72-gd.x86_64	7.2.30-1.22.amzn1	amzn-updates
-----------------	-------------------	--------------

Use o comando a seguir para instalar uma versão específica da biblioteca de desenhos gráficos PHP (por exemplo, versão 7.2) no Amazon Linux AMI:

```
[ec2-user ~]$ sudo yum install php72-gd
```

Para corrigir as permissões de arquivos para o Apache Web Server

Algumas das características disponíveis no WordPress exigem acesso de gravação à raiz do documento do Apache (como carregar mídia pelas telas de Administração). Se você não tiver feito isso, aplique as associações e permissões de grupo a seguir (conforme descrito em mais detalhes no [tutorial do servidor web LAMP \(p. 50\)](#)).

1. Conceda a propriedade do arquivo de /var/www e seu conteúdo para o usuário apache.

```
[ec2-user ~]$ sudo chown -R apache /var/www
```

2. Conceda a propriedade do grupo do /var/www e seu conteúdo para o grupo do apache.

```
[ec2-user ~]$ sudo chgrp -R apache /var/www
```

3. Altere as permissões do diretório do /var/www e de seus subdiretórios para adicionar permissões de gravação do grupo e definir o ID do grupo em subdiretórios futuros.

```
[ec2-user ~]$ sudo chmod 2775 /var/www
[ec2-user ~]$ find /var/www -type d -exec sudo chmod 2775 {} \;
```

4. Altere recursivamente as permissões de arquivo do /var/www e de seus subdiretórios para adicionar permissões de gravação.

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
```

5. Reinicie o Apache Web Server para pegar o grupo e as permissões novas.

- Amazon Linux 2

```
[ec2-user ~]$ sudo systemctl restart httpd
```

- AMI do Amazon Linux

```
[ec2-user ~]$ sudo service httpd restart
```

### Como executar o script de instalação do WordPress com o Amazon Linux 2

Você está pronto para instalar o WordPress. Os comandos usados por você dependem do sistema operacional. Os comandos deste procedimento são destinados ao uso com o Amazon Linux 2. Use o procedimento seguinte com a AMI do Amazon Linux.

1. Use o comando systemctl para garantir que httpd e os serviços do banco de dados sejam iniciados a cada inicialização do sistema.

```
[ec2-user ~]$ sudo systemctl enable httpd && sudo systemctl enable mariadb
```

2. Verifique se o servidor do banco de dados está em execução.

```
[ec2-user ~]$ sudo systemctl status mariadb
```

Se o serviço do banco de dados não está em execução, inicie-o.

```
[ec2-user ~]$ sudo systemctl start mariadb
```

3. Verifique se o Apache Web Server (httpd) está sendo executado.

```
[ec2-user ~]$ sudo systemctl status httpd
```

Se o serviço httpd não estiver sendo executado, inicie-o.

```
[ec2-user ~]$ sudo systemctl start httpd
```

4. Em um navegador da web, insira o URL do blog do WordPress (o endereço DNS público para sua instância ou esse endereço seguido pela pasta blog). Você deve visualizar o script de instalação do WordPress. Forneça as informações necessárias segundo a instalação do WordPress. Escolha Install WordPress (Instalar WordPress) para concluir a instalação. Para obter mais informações, consulte [Etapa 5: Executar o script de instalação](#) no site do WordPress.

### Como executar o script de instalação do WordPress com a AMI do Amazon Linux

1. Use o comando chkconfig para garantir que httpd e os serviços do banco de dados sejam iniciados a cada inicialização do sistema.

```
[ec2-user ~]$ sudo chkconfig httpd on && sudo chkconfig mysqld on
```

2. Verifique se o servidor do banco de dados está em execução.

```
[ec2-user ~]$ sudo service mysqld status
```

Se o serviço do banco de dados não está em execução, inicie-o.

```
[ec2-user ~]$ sudo service mysqld start
```

3. Verifique se o Apache Web Server (`httpd`) está sendo executado.

```
[ec2-user ~]$ sudo service httpd status
```

Se o serviço `httpd` não estiver sendo executado, inicie-o.

```
[ec2-user ~]$ sudo service httpd start
```

4. Em um navegador da web, insira o URL do blog do WordPress (o endereço DNS público para sua instância ou esse endereço seguido pela pasta `blog`). Você deve visualizar o script de instalação do WordPress. Forneça as informações necessárias segundo a instalação do WordPress. Escolha Install WordPress (Instalar WordPress) para concluir a instalação. Para obter mais informações, consulte [Etapa 5: Executar o script de instalação](#) no site do WordPress.

## Próximas etapas

Depois de testar seu blog do WordPress, é recomendável atualizar sua configuração.

### Usar um nome de domínio personalizado

Se você tiver um nome de domínio associado ao endereço EIP da sua instância do EC2, pode configurar o blog para usar esse nome em vez do endereço DNS público do EC2. Para obter mais informações, consulte [Alterar o URL do site](#) no site do WordPress.

### Configurar seu blog

Você pode configurar seu blog para usar diferentes [temas](#) e [plug-ins](#) e oferecer uma experiência mais personalizada para seus leitores. Contudo, às vezes o processo de instalação pode dar errado, fazendo com que você perca o blog inteiro. Recomendamos veementemente que você crie um backup da imagem de máquina da Amazon (AMI) de sua instância antes de tentar instalar quaisquer temas ou plug-ins, de forma que consiga restaurar o blog se algo der errado durante a instalação. Para obter mais informações, consulte [Criar sua própria AMI \(p. 73\)](#).

### Aumentar a capacidade

Se seu blog do WordPress ficar popular e você precisar de mais poder computacional ou armazenamento, considere as etapas a seguir:

- Expanda o espaço de armazenamento na sua instância. Para obter mais informações, consulte [Volumes elásticos do Amazon EBS \(p. 1405\)](#).
- Mova o banco de dados MySQL para o [Amazon RDS](#) para aproveitar a capacidade de dimensionamento que o serviço oferece.

### Melhore a performance de rede do tráfego da Internet

Se você espera que seu blog gere tráfego de usuários localizados em todo o mundo, considere o [AWSGlobal Accelerator](#). O Global Accelerator ajuda você a obter menor latência, melhorando a performance do tráfego da Internet entre os dispositivos cliente de seus usuários e a aplicação WordPress em execução na AWS. O Global Accelerator usa a [rede global da AWS](#) para direcionar o tráfego a um endpoint íntegro da aplicação na região da AWS mais próxima do cliente.

### Saiba mais sobre o WordPress

---

Para obter informações sobre o WordPress, consulte a documentação de ajuda do WordPress Codex em <http://codex.wordpress.org/>. Para obter mais informações sobre como solucionar problemas de instalação, acesse <https://wordpress.org/support/article/how-to-install-wordpress/#common-installation-problems>. Para obter informações sobre como tornar o blog do WordPress mais seguro, acesse <https://wordpress.org/support/article/hardening-wordpress/>. Para obter informações sobre como manter o blog do WordPress atualizado, acesse <https://wordpress.org/support/article/updating-wordpress/>.

## Ajuda! Meu nome DNS público mudou e agora meu blog não está funcionando

A sua instalação do WordPress é configurada automaticamente usando o endereço DNS público da sua instância do EC2. Se você parar e reiniciar a instância, as alterações no endereço DNS público (a menos que estejam associadas a um endereço IP elástico) e seu blog não funcionarão mais, pois ele faz referência a recursos em um endereço que não existe mais (ou é atribuído a outra instância do EC2). Uma descrição mais detalhada do problema e várias soluções possíveis estão descritas em <https://wordpress.org/support/article/changing-the-site-url/>.

Se isso tiver acontecido à sua instalação do WordPress, você pode conseguir recuperar o blog com o procedimento abaixo, usando a interface de linha de comando wp-cli para WordPress.

Para alterar a URL do site do WordPress com wp-cli

1. Conecte-se à sua instância do EC2 com SSH.
2. Anote o URL do site antigo e do site novo para sua instância. O URL do site antigo provavelmente é o nome DNS público da sua instância do EC2 ao instalar o WordPress. O URL do novo site é o nome DNS público atual da sua instância do EC2. Se você não tiver certeza da URL do site antigo, pode usar o curl para encontrá-la com o seguinte comando.

```
[ec2-user ~]$ curl localhost | grep wp-content
```

Você deve visualizar referências ao nome DNS público antigo na saída, que terá a seguinte aparência (URL do site antigo em vermelho):

```
<script type='text/javascript' src='http://ec2-52-8-139-223.us-west-1.compute.amazonaws.com/wp-content/themes/twentyfifteen/js/functions.js?ver=20150330'></script>
```

3. Faça download do wp-cli com o seguinte comando.

```
[ec2-user ~]$ curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar
```

4. Pesquise e substitua o URL do site antigo na instalação do WordPress pelo comando a seguir. Substitua os URLs dos sites novo e antigo para sua instância do EC2 e o caminho para sua instalação do WordPress (geralmente /var/www/html ou /var/www/html/blog).

```
[ec2-user ~]$ php wp-cli.phar search-replace 'old_site_url' 'new_site_url' --path=/path/to/wordpress/installation --skip-columns=guid
```

5. Em um navegador, insira o URL de novo site do blog do WordPress para verificar se o site está funcionando corretamente. Se não estiver, consulte <https://wordpress.org/support/article/changing-the-site-url/> e <https://wordpress.org/support/article/how-to-install-wordpress/#common-installation-problems> para obter mais informações.

# Tutorial: Instalar um servidor web LAMP no Amazon Linux AMI

Os procedimentos a seguir ajudam a instalar o servidor web Apache com suporte do PHP e do MySQL na instância do Amazon Linux (às vezes denominado servidor web LAMP ou pilha LAMP). Você pode usar esse servidor para hospedar um site estático ou para implantar um aplicativo PHP dinâmico que lê e grava informações em um banco de dados.

## Important

Se você estiver tentando configurar um servidor web LAMP em uma distribuição diferente, como Ubuntu ou Red Hat Enterprise Linux, este tutorial não funcionará. Em Amazon Linux 2, consulte [Tutorial: Instalar um servidor web LAMP no Amazon Linux 2 \(p. 15\)](#). Para o Ubuntu, consulte a seguinte documentação da comunidade do Ubuntu: [ApacheMySQLPHP](#). Para outras distribuições, consulte a documentação específica.

Opção: concluir este tutorial usando a automação

Para concluir este tutorial usando a automação do AWS Systems Manager em vez das tarefas a seguir, execute o documento de automação [Docs-InstallALAMPServer-AL da AWS](#).

## Tarefas

- [Etapa 1: Preparar o servidor LAMP \(p. 50\)](#)
- [Etapa 2: Testar o servidor LAMP \(p. 54\)](#)
- [Etapa 3: Proteger o servidor do banco de dados \(p. 55\)](#)
- [Etapa 4: \(opcional\) instalar o phpMyAdmin \(p. 56\)](#)
- [Troubleshoot \(p. 59\)](#)
- [Tópicos relacionados \(p. 60\)](#)

## Etapa 1: Preparar o servidor LAMP

### Prerequisites

Este tutorial pressupõe que você já tenha executado uma nova instância usando a Amazon Linux AMI com um nome DNS público acessível pela internet. Para obter mais informações, consulte [Etapa 1: executar uma instância \(p. 10\)](#). Você também precisa ter configurado o security group para permitir conexões SSH (porta 22), HTTP (porta 80) e HTTPS (porta 443). Para obter mais informações sobre esses pré-requisitos, consulte [Autorizar tráfego de entrada para suas instâncias do Linux \(p. 1205\)](#).

Para instalar e iniciar o servidor web do LAMP com a Amazon Linux AMI

1. [Conecte-se à sua instância \(p. 11\)](#).
2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. Esse processo pode levar alguns minutos, mas é importante ter certeza de que você tem as atualizações de segurança e correções de bug mais recentes.

A opção `-y` instala as atualizações sem solicitar confirmação. Para examinar as atualizações antes da instalação, você pode omitir essa opção.

```
[ec2-user ~]$ sudo yum update -y
```

3. Agora que sua instância é atual, você pode instalar o servidor web Apache, o MySQL e os pacotes de software do PHP.

### Important

Alguns aplicativos podem não ser compatíveis com o seguinte ambiente de software recomendado. Antes de instalar esses pacotes, verifique se os aplicativos LAMP são compatíveis com eles. Se houver algum problema, talvez seja necessário instalar um ambiente alternativo. Para obter mais informações, consult [O software aplicativo compatível que desejo executar no meu servidor é incompatível com a versão PHP instalada ou outro software \(p. 59\)](#)

Use o comando yum install para instalar os vários pacotes de software e todas as dependências relacionadas ao mesmo tempo.

```
[ec2-user ~]$ sudo yum install -y httpd24 php72 mysql57-server php72-mysqlnd
```

Se receber o erro No package *package-name* available, isso significa que sua instância não foi executada com a Amazon Linux AMI (talvez você esteja usando o Amazon Linux 2). Você pode visualizar sua versão do Amazon Linux com o comando a seguir.

```
cat /etc/system-release
```

4. Inicie o servidor web Apache.

```
[ec2-user ~]$ sudo service httpd start
Starting httpd: [ OK ]
```

5. Use o comando chkconfig para configurar o servidor web Apache para iniciar em cada inicialização do sistema.

```
[ec2-user ~]$ sudo chkconfig httpd on
```

O comando chkconfig não fornece nenhuma mensagem de confirmação quando você o usa com êxito para habilitar um serviço.

Você pode verificar se httpd está ativo executando o seguinte comando:

```
[ec2-user ~]$ chkconfig --list httpd
httpd      0:off  1:off  2:on   3:on   4:on   5:on   6:off
```

Aqui, httpd é on nos runlevels 2, 3, 4 e 5 (que é o que você deseja ver).

6. Adicione uma regra de segurança para permitir conexões HTTP de entrada (porta 80) na instância caso você ainda não tenha feito isso. Por padrão, um grupo de segurança launch-wizard-N foi configurado para a instância durante a inicialização. Esse grupo contém uma única regra para permitir conexões SSH.
  - a. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
  - b. Escolha Instances (Instâncias) e selecione a instância.
  - c. Na guia Security (Segurança), exiba as regras de entrada. Você deve ver a seguinte regra:

Port range	Protocol	Source
22	tcp	0.0.0.0/0

## Warning

Usar `0.0.0.0/0` permite que todos os endereços IPv4 acessem sua instância usando o SSH. 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.

- d. Escolha o link do grupo de segurança. Usando os procedimentos contidos em [Adicionar regras a um grupo de segurança \(p. 1233\)](#), adicione uma nova regra de segurança de entrada com os seguintes valores:
  - Type (Tipo): HTTP
  - Protocol (Protocolo): TCP
  - Port Range: 80
  - Source (Origem): personalizado
7. Teste o servidor web. Em um navegador, digite o endereço DNS público (ou o endereço IP público) de sua instância. Você pode obter o endereço DNS público para sua instância usando o console do Amazon EC2. Se não houver conteúdo em `/var/www/html`, você deverá verificar a página de teste do Apache. Quando você adiciona conteúdo ao diretório base, o conteúdo aparece no endereço DNS público da instância em vez desta página de teste.

Verifique se o grupo de segurança da instância contém uma regra para permitir o tráfego HTTP na porta 80. Para obter mais informações, consulte [Adicionar regras a um grupo de segurança \(p. 1233\)](#).

Se você não estiver usando o Amazon Linux, poderá ser necessário configurar o firewall na instância para permitir essas conexões. Para obter mais informações sobre como configurar o firewall, consulte a documentação de sua distribuição específica.

## Amazon Linux AMI Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the web server installed at this site is working properly, but has not yet been configured.

### If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting `www.example.com`, you should send e-mail to `"webmaster@example.com"`.

The [Amazon Linux AMI](#) is a supported and maintained Linux image provided by [Amazon Web Services](#) for use on [Amazon Elastic Compute Cloud \(Amazon EC2\)](#). It is designed to provide a stable, secure, and high performance execution environment for applications running on [Amazon EC2](#). It also includes packages that enable easy integration with [AWS](#), including launch configuration tools and many popular AWS libraries and tools. [Amazon Web Services](#) provides ongoing security and maintenance updates to all instances running the [Amazon Linux AMI](#). The [Amazon Linux AMI](#) is provided at no additional charge to [Amazon EC2 users](#).

### If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `/etc/httpd/conf.d/welcome.conf`.

You are free to use the images below on Apache and Amazon Linux AMI powered HTTP servers. Thanks for using Apache and the Amazon Linux AMI!



O httpd do Apache é usado para os arquivos que são mantidos em um diretório chamado raiz de documentos do Apache. O diretório raiz de documentos Apache do Amazon Linux é /var/www/html, que, por padrão, é de propriedade da raiz.

```
[ec2-user ~]$ ls -l /var/www
total 16
drwxr-xr-x 2 root root 4096 Jul 12 01:00 cgi-bin
drwxr-xr-x 3 root root 4096 Aug 7 00:02 error
drwxr-xr-x 2 root root 4096 Jan 6 2012 html
drwxr-xr-x 3 root root 4096 Aug 7 00:02 icons
drwxr-xr-x 2 root root 4096 Aug 7 21:17 noindex
```

Para permitir que a conta do ec2-user manipule arquivos nesse diretório, você deve modificar a propriedade e as permissões do diretório. Existem diversas maneiras de realizar essa tarefa. Neste tutorial, você adiciona o usuário ec2-user ao grupo apache para dar ao grupo apache a propriedade do diretório /var/www e atribuir permissões de gravação ao grupo.

Para definir permissões de arquivo

1. Adicione o usuário (neste caso, o ec2-user) ao grupo do apache.

```
[ec2-user ~]$ sudo usermod -a -G apache ec2-user
```

2. Faça logout e login novamente para selecionar o novo grupo verifique sua associação.

- a. Faça logout (use o comando exit ou feche a janela do terminal):

```
[ec2-user ~]$ exit
```

- b. Para verificar sua associação no grupo apache, reconecte-se à instância e execute o comando a seguir:

```
[ec2-user ~]$ groups
ec2-user wheel apache
```

3. Altere a propriedade do grupo do /var/www e seu conteúdo para o grupo do apache.

```
[ec2-user ~]$ sudo chown -R ec2-user:apache /var/www
```

4. Para adicionar as permissões de gravação do grupo e definir o ID do grupo nos subdiretórios futuros, altere as permissões de diretório de /var/www e de seus subdiretórios.

```
[ec2-user ~]$ sudo chmod 2775 /var/www
[ec2-user ~]$ find /var/www -type d -exec sudo chmod 2775 {} \;
```

5. Para adicionar permissões de gravação do grupo, altere recursivamente as permissões de arquivo de /var/www e de seus subdiretórios:

```
[ec2-user ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;
```

Agora, ec2-user (e outros todos os futuros do grupo apache) poderão adicionar, excluir e editar arquivos na raiz do documento Apache, permitindo que você adicione conteúdo, como um site estático ou um aplicativo PHP.

(Opcional) Proteger o servidor web

Um servidor web que executa o protocolo HTTP não fornece nenhuma segurança de transporte para os dados que envia ou recebe. Quando você se conecta a um servidor HTTP usando um navegador da web, as URLs que você acessa, o conteúdo de páginas da web recebido e o conteúdo (incluindo senhas) de todos os formulários HTML enviado por você ficam visíveis para os espiões em qualquer ponto da rede. A melhor prática para proteger o servidor web é instalar suporte para HTTPS (HTTP seguro), que protege os dados por meio de criptografia SSL/TLS.

Para obter informações sobre como habilitar o HTTPS no servidor, consulte [Tutorial: Configurar o SSL/TLS com a AMI do Amazon Linux \(p. 60\)](#).

## Etapa 2: Testar o servidor LAMP

Se o servidor estiver instalado e em execução, e suas permissões de arquivo estiverem definidas corretamente, a conta do `ec2-user` poderá criar um arquivo PHP no diretório `/var/www/html` disponível na Internet.

Para testar o servidor web do LAMP

1. Crie um arquivo PHP no diretório base do Apache.

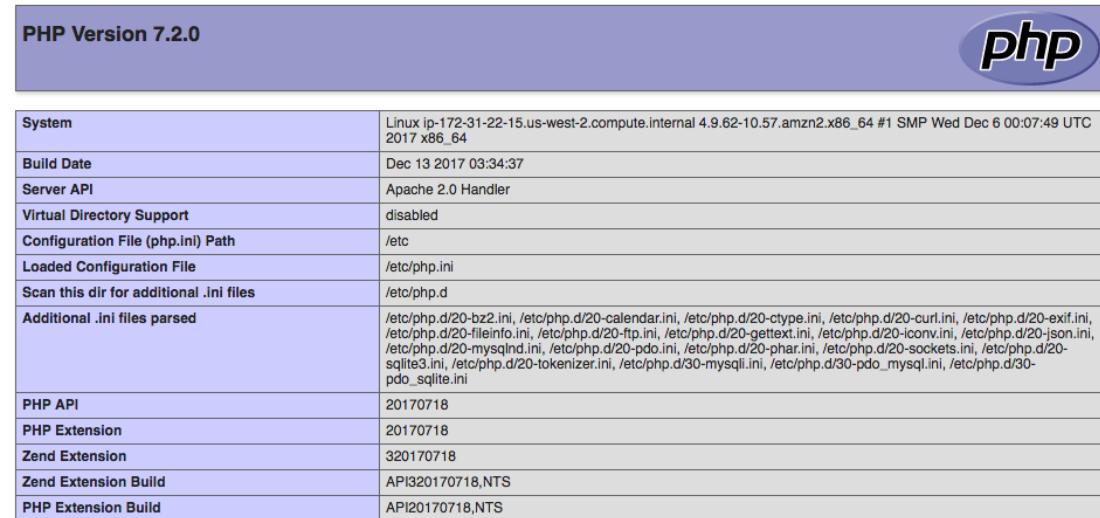
```
[ec2-user ~]$ echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Se você receber o erro "Permissão negada" ao tentar executar esse comando, tente fazer logout e login novamente para obter as permissões corretas do grupo que você configurou em [Etapa 1: Preparar o servidor LAMP \(p. 50\)](#).

2. Em um navegador da web, digite a URL do arquivo que você acabou de criar. Essa URL é o endereço DNS público da instância seguido por uma barra e o nome do arquivo. Por exemplo:

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Você deve ver a página de informações do PHP:



PHP Version 7.2.0	
System	Linux ip-172-31-22-15.us-west-2.compute.internal 4.9.62-10.57.amzn2.x86_64 #1 SMP Wed Dec 6 00:07:49 UTC 2017 x86_64
Build Date	Dec 13 2017 03:34:37
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-ctype.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-fileinfo.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-json.ini, /etc/php.d/20-mysqlind.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-sockets.ini, /etc/php.d/20-sqlite3.ini, /etc/php.d/20-tokenizer.ini, /etc/php.d/30-mysqli.ini, /etc/php.d/30-pdo_mysql.ini, /etc/php.d/30-pdo_sqlite.ini
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS

Se você não vir essa página, verifique se o arquivo `/var/www/html/phpinfo.php` foi criado corretamente na etapa anterior. Você também pode verificar se todos os pacotes necessários foram instalados com o comando a seguir. As versões de pacote na segunda coluna não precisam corresponder a esse exemplo de saída.

```
[ec2-user ~]$ sudo yum list installed httpd24 php72 mysql57-server php72-mysqlnd
```

```
Loaded plugins: priorities, update-motd, upgrade-helper
Installed Packages
httpd24.x86_64           2.4.25-1.68.amzn1          @amzn-
updates
mysql56-server.x86_64     5.6.35-1.23.amzn1          @amzn-
updates
php70.x86_64              7.0.14-1.20.amzn1          @amzn-
updates
php70-mysqlnd.x86_64      7.0.14-1.20.amzn1          @amzn-
updates
```

Se alguns dos pacotes necessários não estiverem listados na saída, instale-os usando o comando `sudo yum install package`.

3. Exclua o arquivo `phpinfo.php`. Embora essas informações possam ser úteis, elas não devem ser transmitidas pela Internet por motivos de segurança.

```
[ec2-user ~]$ rm /var/www/html/phpinfo.php
```

## Etapa 3: Proteger o servidor do banco de dados

A instalação padrão do servidor MySQL tem vários recursos que são bons para teste e desenvolvimento, mas devem ser desabilitados ou removidos em servidores de produção. O comando `mysql_secure_installation` orienta você durante o processo de configuração de uma senha raiz e da remoção de recursos não seguros da instalação. Mesmo que você não esteja planejando usar o servidor MySQL, é recomendável executar este procedimento.

Para proteger o servidor do banco de dados

1. Inicie o servidor MySQL.

```
[ec2-user ~]$ sudo service mysqld start
Initializing MySQL database:
...
PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
...
Starting mysqld:                                         [    OK    ]
```

2. Executar `mysql_secure_installation`.

```
[ec2-user ~]$ sudo mysql_secure_installation
```

- Quando solicitado, digite uma senha para a conta raiz.
  - Digite a senha raiz atual. Por padrão, a conta raiz não tem uma senha definida. Pressione Enter.
  - Digite **y** para definir uma senha e digite uma senha segura duas vezes. Para obter mais informações sobre como criar uma senha segura, consulte <https://identitysafe.norton.com/password-generator/>. Armazene essa senha em um lugar seguro.

A configuração de uma senha raiz para o MySQL é somente a medida mais básica para proteger seu banco de dados. Ao criar ou instalar um aplicativo controlado por banco de dados, geralmente, você cria um usuário de serviço de banco para esse aplicativo e evita usar a conta raiz para qualquer coisa que não seja a administração do banco de dados.

- Digit **y** para remover as contas de usuários anônimos.

- c. Digite **y** para desabilitar o recurso de login remoto da raiz.
- d. Digite **y** para remover o banco de dados de teste.
- e. Digite **y** para recarregar as tabelas de privilégios e salvar suas alterações.
3. (Opcional) Se você não pretende usar o servidor MySQL imediatamente, interrompa-o. Você poderá reiniciá-lo quando precisar dele novamente.

```
[ec2-user ~]$ sudo service mysqld stop
Stopping mysqld: [OK]
```

4. (Opcional) Se você quiser que o servidor MySQL seja iniciado a cada inicialização, digite o comando a seguir.

```
[ec2-user ~]$ sudo chkconfig mysqld on
```

Agora você deve ter um servidor web do LAMP totalmente funcional. Se adicionar conteúdo ao diretório base do Apache em `/var/www/html`, você deverá poder visualizar esse conteúdo no endereço DNS público de sua instância.

## Etapa 4: (opcional) instalar o phpMyAdmin

Para instalar o phpMyAdmin

O [phpMyAdmin](#) é uma ferramenta de gerenciamento de banco de dados baseada na web que você pode usar para visualizar e editar os bancos de dados MySQL na instância do EC2. Siga as etapas a seguir para instalar e configurar o phpMyAdmin em sua instância do Amazon Linux.

### Important

Não recomendamos usar o phpMyAdmin para acessar um servidor LAMP, a menos que você tenha habilitado o SSL/TLS no Apache. Caso contrário, sua senha de administrador de banco de dados e outros dados serão transmitidos de forma desprotegida pela Internet. Para ver as recomendações de segurança dos desenvolvedores, consulte [Securing your phpMyAdmin installation](#).

### Note

No momento, o sistema de gerenciamento de pacotes do Amazon Linux não oferece suporte à instalação automática do phpMyAdmin em um ambiente PHP 7. Este tutorial descreve como instalar o phpMyAdmin manualmente.

1. Inicie a sessão na instância do EC2 usando o SSH.
2. Instale as dependências necessárias.

```
[ec2-user ~]$ sudo yum install php72-mbstring.x86_64 -y
```

3. Reinicie o Apache.

```
[ec2-user ~]$ sudo service httpd restart
Stopping httpd: [OK]
Starting httpd: [OK]
```

4. Navegue até o diretório base do Apache em `/var/www/html`.

```
[ec2-user ~]$ cd /var/www/html
[ec2-user html]$
```

5. Selecione um pacote de origem para a versão mais recente do phpMyAdmin em <https://www.phpmyadmin.net/downloads>. Para fazer download do arquivo diretamente para a instância, copie o link e cole-o em um comando wget, como neste exemplo:

```
[ec2-user html]$ wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz
```

6. Crie uma pasta phpMyAdmin e extraia o pacote dela com o comando a seguir.

```
[ec2-user html]$ mkdir phpMyAdmin && tar -xvzf phpMyAdmin-latest-all-languages.tar.gz -C phpMyAdmin --strip-components 1
```

7. Exclua o tarball *phpMyAdmin-latest-all-languages.tar.gz*.

```
[ec2-user html]$ rm phpMyAdmin-latest-all-languages.tar.gz
```

8. (Opcional) Se o servidor MySQL não estiver em execução, inicie-o agora.

```
[ec2-user ~]$ sudo service mysqld start
Starting mysqld: [ OK ]
```

9. Em um navegador da web, digite a URL da instalação do phpMyAdmin. Essa URL é o endereço DNS público (ou o endereço IP público) da instância seguido por uma barra e o nome do diretório de instalação. Por exemplo:

```
http://my.public.dns.amazonaws.com/phpMyAdmin
```

Você deve ver a página de login do phpMyAdmin:



10. Inicie a sessão na instalação do phpMyAdmin com o nome de usuário `root` e a senha raiz do MySQL criada anteriormente.

A instalação ainda deve ser configurada antes que você a coloque em serviço. Para configurar o phpMyAdmin, você pode [criar manualmente um arquivo de configuração, usar o console de configuração](#) ou combinar ambas as abordagens.

Para obter informações sobre o uso do phpMyAdmin, consulte o [Guia do usuário do phpMyAdmin](#).

## Troubleshoot

Esta seção oferece sugestões para resolver problemas comuns que você pode encontrar ao configurar um novo servidor do LAMP.

### Não é possível conectar ao servidor usando um navegador da web.

Execute as seguintes verificações para ver se o servidor da web do Apache está em execução e acessível.

- O servidor web está em execução?

Você pode verificar se httpd está ativo executando o seguinte comando:

```
[ec2-user ~]$ chkconfig --list httpd
httpd           0:off    1:off    2:on     3:on     4:on     5:on     6:off
```

Aqui, httpd é on nos runlevels 2, 3, 4 e 5 (que é o que você deseja ver).

Se o processo httpd não estiver em execução, repita as etapas descritas em [Etapa 1: Preparar o servidor LAMP \(p. 50\)](#).

- O firewall está configurado corretamente?

Verifique se o grupo de segurança da instância contém uma regra para permitir o tráfego HTTP na porta 80. Para obter mais informações, consulte [Adicionar regras a um grupo de segurança \(p. 1233\)](#).

### O software aplicativo compatível que desejo executar no meu servidor é incompatível com a versão PHP instalada ou outro software

Este tutorial recomenda instalar as versões mais atualizadas do Servidor HTTP Apache, do PHP e do MySQL. Antes de instalar um aplicativo LAMP adicional, verifique seus requisitos para ter a certeza de que ele é compatível com o ambiente instalado. Se a versão mais recente do PHP não for compatível, será possível (e totalmente seguro) fazer downgrade para uma configuração anterior com suporte. Você também pode instalar mais de uma versão do PHP em paralelo, o que resolverá alguns problemas de compatibilidade com um mínimo de esforço. Para obter informações sobre como configurar uma preferência entre várias versões do PHP, consulte [Notas de release do Amazon Linux AMI 2016.09](#).

#### Como fazer downgrade

A versão anterior testada deste tutorial chamada para os seguintes pacotes LAMP principais:

- httpd24
- php56
- mysql55-server
- php56-mysqlnd

Se você já tiver instalado os pacotes mais recentes como recomendado no início deste tutorial, primeiro desinstale esses pacotes e outras dependências, conforme especificado a seguir:

```
[ec2-user ~]$ sudo yum remove -y httpd24 php72 mysql57-server php72-mysqlnd perl-DBD-
MySQL57
```

Em seguida, instale o ambiente de substituição:

```
[ec2-user ~]$ sudo yum install -y httpd24 php56 mysql55-server php56-mysqlnd
```

Se você decidir fazer a atualização para o ambiente recomendado mais tarde, deverá primeiro remover os pacotes e as dependências personalizados:

```
[ec2-user ~]$ sudo yum remove -y httpd24 php56 mysql55-server php56-mysqlnd perl-DBD-MySQL56
```

Agora você pode instalar os pacotes mais recentes, como descrito anteriormente.

## Tópicos relacionados

Para obter mais informações sobre como transferir arquivos para a instância ou como instalar um blog do WordPress no servidor web, consulte a documentação a seguir:

- [Transferir arquivos uma sua instância do Linux usando WinSCP \(p. 555\)](#)
- [Transfira arquivos para instâncias do Linux usando um cliente SCP \(p. 539\)](#)
- [Tutorial: Hospedar um blog do WordPress no Amazon Linux 2 \(p. 40\)](#)

Para obter mais informações sobre os comandos e o software usados neste tutorial, consulte as seguintes páginas da web:

- Servidor web Apache: <http://httpd.apache.org/>
- Servidor do banco de dados MySQL: <http://www.mysql.com/>
- Linguagem de programação PHP: <http://php.net/>
- O comando chmod: <https://en.wikipedia.org/wiki/Chmod>
- O comando chown: <https://en.wikipedia.org/wiki/Chown>

Para obter mais informações sobre como registrar um nome de domínio para o servidor web ou transferir um nome de domínio existente para este host, consulte [Como criar e migrar domínios e subdomínios para o Amazon Route 53](#) no Guia do desenvolvedor do Amazon Route 53.

## Tutorial: Configurar o SSL/TLS com a AMI do Amazon Linux

O Secure Sockets Layer/Transport Layer Security (SSL/TLS) cria um canal criptografado entre um servidor web e um cliente web que protege os dados em trânsito contra espionagem. Este tutorial explica como adicionar suporte manualmente para o SSL/TLS em uma instância do EC2 com o servidor web do Apache e a AMI do Amazon Linux. Este tutorial pressupõe que você não esteja usando um平衡ador de carga. Se você estiver usando Elastic Load Balancing, poderá optar por configurar o descarregamento do SSL no balanceador de carga, usando, em vez disso, um certificado do [AWS Certificate Manager](#).

Por motivos históricos, a criptografia na Web é conhecida simplesmente como SSL. Embora os navegadores da web ainda ofereçam suporte ao SSL, o protocolo sucessor, o TLS, é menos vulnerável a ataques. A AMI do Amazon Linux desabilita o suporte no lado do servidor a todas as versões do SSL por padrão. Os [órgãos de normas de segurança](#) consideram o TLS 1.0 inseguro, e tanto o TLS 1.0 quanto o TLS 1.1 estão prestes a ser formalmente [suspenso](#)s pelo IETF. Este tutorial contém orientações baseadas exclusivamente na ativação do TLS 1.2. (Existe um protocolo TLS 1.3 mais novo em formato de rascunho,

mas ele não é compatível com o Amazon Linux.) Para obter mais informações sobre os padrões de criptografia atualizados, consulte [RFC 7568](#) e [RFC 8446](#).

Este tutorial refere-se à criptografia da web moderna simplesmente como TLS.

#### Important

Esses procedimentos são destinados à AMI do Amazon Linux. Se estiver tentando configurar um servidor web LAMP em uma instância com distribuição diferente, alguns procedimentos deste tutorial poderão não funcionar para você. Em Amazon Linux 2, consulte [Tutorial: configurar o SSL/TLS no Amazon Linux 2 \(p. 25\)](#). Para o Ubuntu, consulte a seguinte documentação da comunidade do Ubuntu: [ApacheMySQLPHP](#). Para o Red Hat Enterprise Linux, consulte: [Como configurar o Servidor Web Apache HTTP](#). Para outras distribuições, consulte a documentação específica.

#### Tópicos

- [Prerequisites \(p. 61\)](#)
- [Etapa 1: habilitar o TLS no servidor \(p. 61\)](#)
- [Etapa 2: obter um certificado assinado por uma CA \(p. 63\)](#)
- [Etapa 3: testar e intensificar a configuração de segurança \(p. 68\)](#)
- [Troubleshoot \(p. 70\)](#)

## Prerequisites

Antes de começar este tutorial, conclua as seguintes etapas:

- Execute uma instância baseada em EBS usando a AMI do Amazon Linux. Para obter mais informações, consulte [Etapa 1: executar uma instância \(p. 10\)](#).
- Configure seu security group para permitir que sua instância aceite conexões nas seguintes portas TCP:
  - SSH (porta 22)
  - HTTP (porta 80)
  - HTTPS (porta 443)

Para obter mais informações, consulte [Autorizar tráfego de entrada para suas instâncias do Linux \(p. 1205\)](#).

- Instale o servidor da web do Apache. Para obter as instruções passo a passo, consulte [Tutorial: como instalar um servidor da web LAMP no Amazon Linux \(p. 50\)](#). Somente o pacote http24 e suas dependências são necessários. Você pode ignorar as instruções que envolvem PHP e MySQL.
- Para identificar e autenticar sites, a infraestrutura de chave pública (PKI) do TLS depende do Domain Name System (DNS). Para usar sua instância do EC2 e hospedar um site público, você precisa registrar um nome de domínio para seu servidor da web ou transferir um nome de domínio existente para o host do Amazon EC2. Há vários serviços de registro de domínio e de hospedagem DNS de terceiros disponíveis para isso, ou você pode usar o [Amazon Route 53](#).

## Etapa 1: habilitar o TLS no servidor

Este procedimento auxilia no processo de configuração do TLS no Amazon Linux com um certificado digital autoassinado.

#### Note

Um certificado autoassinado é aceitável para testes, mas não para produção. Quando você expõe seu certificado autoassinado na Internet, os visitantes de seu site recebem avisos de segurança.

Para habilitar o TLS em um servidor

1. [Conecte-se à sua instância \(p. 11\)](#) e confirme se o Apache está em execução.

```
[ec2-user ~]$ sudo service httpd status
```

Se necessário, inicie o Apache.

```
[ec2-user ~]$ sudo service httpd start
```

2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. Esse processo pode levar alguns minutos, mas é importante ter certeza de que você tem as atualizações de segurança e correções mais recentes.

Note

A opção `-y` instala as atualizações sem solicitar confirmação. Para examinar as atualizações antes da instalação, você pode omitir essa opção.

```
[ec2-user ~]$ sudo yum update -y
```

3. Agora que sua instância está atualizada, adicione o suporte ao TLS instalando o módulo `mod_ssl` do Apache:

```
[ec2-user ~]$ sudo yum install -y mod24_ssl
```

Sua instância agora possui os seguintes arquivos que você usará para configurar seu servidor seguro e criar um certificado para teste:

`/etc/httpd/conf.d/ssl.conf`

O arquivo de configuração para `mod_ssl`. Contém as "diretrizes" que informam ao Apache onde encontrar chaves de criptografia e certificados, as versões do protocolo TLS a serem permitidas e as cifras de criptografia a serem aceitas.

`/etc/pki/tls/private/localhost.key`

Uma chave privada de RSA de 2048 bits gerada automaticamente para seu host do Amazon EC2. Durante a instalação, o OpenSSL usou essa chave para gerar um certificado autoassinado do host, e você também pode usar essa chave para gerar uma solicitação de assinatura de certificado (CSR) a ser enviada a uma autoridade de certificação (CA).

`/etc/pki/tls/certs/localhost.crt`

Um certificado de X.509 autoassinado gerado automaticamente para seu servidor de host. Esse certificado é útil para testar se o Apache está configurado corretamente para usar o TLS.

Os arquivos `.key` e `.crt` estão no formato PEM, que consiste em caracteres ASCII codificados em Base64 enquadradados pelas linhas "BEGIN" e "END", como neste exemplo abreviado de um certificado:

```
-----BEGIN CERTIFICATE-----  
MIIEazCCA1OgAwIBAgICWxQwDQYJKoZIhvcNAQELBQAwgbExCzAJBgNVBAYTAi0t  
MRIwEAYDVQQIDA1Tb21lU3RhGUxETAPBgNVBAcMCFNvbWVDaXR5MRkwFwYDVQQK  
DBBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLDBZTb21lT3JnYW5pemF0aW9uYWxV  
bmlOMRkwFwYDVQODDBBpcC0xNzItMzEtMjAtMjM2MSQwIgYJKoZIhvcNAQkBFhVy  
...  
z5rRUE/XzxRLBZ0oWZpNWTXJkQ3uFYH6s/sBwtHpKKZMzOvDedREjNKAvk4ws6F0  
WanXWehT6FisZvB4sTEXXJN2jdw8g+sHGNz8zCoSclknYhHrCVD2vnBlZJKSzvak
```

```
3ZazhBxtQSukFMOnWPP2a0DMMFYUH0d0BQE8sBJxg==  
-----END CERTIFICATE-----
```

Os nomes e as extensões dos arquivos são uma conveniência e não têm efeito sobre a função. Você pode chamar um certificado de `cert.crt`, `cert.pem` ou qualquer outro nome de arquivo, desde que a diretriz relacionada no arquivo `ssl.conf` use o mesmo nome.

**Note**

Ao substituir os arquivos TLS padrão por seus próprios arquivos personalizados, verifique se eles estão no formato PEM.

4. Reinicie o Apache.

```
[ec2-user ~]$ sudo service httpd restart
```

5. Seu servidor da web do Apache agora deve oferecer suporte a HTTPS (HTTP seguro) por meio da porta 443. Teste-o digitando o endereço IP ou o nome do domínio totalmente qualificado de sua instância do EC2 em uma barra de URL de um navegador com o prefixo `https://`. Como você está se conectando a um site com um certificado autoassinado não confiável, o navegador poderá exibir uma série de avisos de segurança.

Ignore os avisos e continue para o site. Se a página de teste padrão do Apache for aberta, a configuração do TLS no servidor estará correta. Todos os dados que passam entre o navegador e o servidor agora estão criptografados com segurança.

Para impedir que os visitantes do site encontrem telas de avisos, você precisa obter um certificado que, além de criptografar, também autentique você publicamente como o proprietário do site.

## Etapa 2: obter um certificado assinado por uma CA

Você pode seguir este processo para obter um certificado assinado por uma CA:

- Gere uma solicitação de assinatura de certificado (CSR) a partir de uma chave privada
- Enviar a CSR para uma autoridade de certificação (CA)
- Obtenha um certificado de host assinado
- Configure o Apache para usá-lo

Um certificado de host TLS X.509 autoassinado é idêntico em termos criptológicos a um certificado assinado por uma CA. A diferença é social, não matemática. Uma CA promete validar, no mínimo, a propriedade de um domínio antes de emitir um certificado para um candidato. Cada navegador da web contém uma lista de CAs confiáveis pelo fornecedor do navegador para fazer isso. Primariamente, um certificado X.509 consiste em uma chave pública, que corresponde à chave privada do servidor, e uma assinatura pela CA que é vinculada criptograficamente à chave pública. Quando um navegador se conecta a um servidor da Web por meio de HTTPS, o servidor apresenta um certificado ao navegador para verificação em sua lista de CAs confiáveis. Se o assinante estiver na lista ou for acessível por meio de uma cadeia de confiança que consiste em outros assinantes confiáveis, o navegador negociará um canal rápido de dados criptografados com o servidor e carregará a página.

Geralmente, os certificados são caros devido ao trabalho envolvido na validação das solicitações, portanto, vale a pena comparar os preços. Algumas CAs oferecem certificados de nível básico gratuitamente. Entre essas CAs, a mais notável é o projeto [Let's Encrypt](#), que também oferece suporte à automação de criação de certificados e ao processo de renovação. Para obter mais informações sobre como usar a Let's Encrypt como sua CA, consulte [Automação de certificados: Let's Encrypt com o Certbot no Amazon Linux 2 \(p. 36\)](#).

Se você planeja oferecer serviços de nível comercial, o [AWS Certificate Manager](#) é uma boa opção.

É importante ter um certificado de host subjacente. Desde 2017, grupos [governamentais](#) e do [setor](#) recomendam usar um tamanho de chave (módulo) mínimo de 2048 bits para chaves de RSA para a proteção de documentos até 2030. O tamanho do módulo padrão gerado pela OpenSSL no Amazon Linux é de 2048 bits, o que significa que a chave existente gerada automaticamente é adequada para uso em um certificado assinado por uma CA. Um procedimento alternativo é descrito a seguir para quem deseja uma chave personalizada, por exemplo, uma chave com um módulo maior ou que use outro algoritmo de criptografia.

As instruções para adquirir certificados de host assinados pela CA não funcionarão, a menos que você possua um domínio DNS registrado e hospedado.

#### Para obter um certificado assinado por uma CA

1. [Conecte-se à sua instância \(p. 11\)](#) e navegue até `/etc/pki/tls/private/`. Esse é o diretório onde a chave privada do servidor para TLS é armazenada. Se você preferir usar sua chave de host existente para gerar a CSR, vá para a Etapa 3.
2. (Opcional) Gerar uma nova chave privada. Estes são alguns exemplos de configurações de chave. Qualquer uma das chaves resultantes funciona com seu servidor web, mas elas variam em como (e quanto) de segurança implementam.
  - Exemplo 1: criar uma chave host de RSA padrão. O arquivo resultante, **custom.key**, é uma chave privada de RSA de 2048 bits.

```
[ec2-user ~]$ sudo openssl genrsa -out custom.key
```

- Exemplo 2: criar uma chave de RSA mais forte com um módulo maior. O arquivo resultante, **custom.key**, é uma chave privada de RSA de 4096 bits.

```
[ec2-user ~]$ sudo openssl genrsa -out custom.key 4096
```

- Exemplo 3: criar uma chave de RSA de 4096 bits criptografada com proteção por senha. O arquivo resultante, **custom.key**, é uma chave privada de RSA de 4096 bits criptografada com a cifra AES-128.

#### Important

A criptografia da chave fornece maior segurança, mas como uma chave criptografada requer uma senha, os serviços que dependem dela não podem ser iniciados automaticamente. Sempre que usar essa chave, você precisará fornecer a senha (no exemplo anterior, "abcde12345") por meio de uma conexão SSH.

```
[ec2-user ~]$ sudo openssl genrsa -aes128 -passout pass:abcde12345 -out custom.key 4096
```

- Exemplo 4: criar uma chave usando uma cifra não RSA. A criptografia RSA pode ser relativamente devagar devido ao tamanho de suas chaves públicas, que são baseadas no produto de dois números primos grandes. No entanto, é possível criar chaves para TLS que usam códigos não RSA. As chaves baseadas em matemática de curvas elípticas são menores e computacionalmente mais rápidas para fornecer um nível de segurança equivalente.

```
[ec2-user ~]$ sudo openssl ecparam -name prime256v1 -out custom.key -genkey
```

O resultado é uma chave privada de curva elíptica de 256 bits que usa prime256v1, uma "curva nomeada" compatível com OpenSSL. A força de criptografia é um pouco maior que uma chave de RSA de 2048 bits, [de acordo com o NIST](#).

### Note

Nem todas as CAs fornecem o mesmo nível de suporte para chaves baseadas em curvas elípticas como para chaves de RSA.

Verifique se a nova chave privada tem a propriedade e permissões altamente restritivas (owner=root, group=root, leitura/gravação para o proprietário somente). Os comandos seriam os seguintes:

```
[ec2-user ~]$ sudo chown root.root custom.key
[ec2-user ~]$ sudo chmod 600 custom.key
[ec2-user ~]$ ls -al custom.key
```

Os comandos acima devem produzir o seguinte resultado:

```
-rw----- root root custom.key
```

Depois de criar e configurar uma chave satisfatória, você pode criar uma CSR.

3. Crie uma CSR usando sua chave preferencial. O exemplo abaixo usa **custom.key**:

```
[ec2-user ~]$ sudo openssl req -new -key custom.key -out csr.pem
```

A OpenSSL abre uma caixa de diálogo e solicita a informação exibida na tabela a seguir. Todos os campos, exceto Common Name (Nome comum), são opcionais para um certificado de host básico validado por domínio.

Nome	Descrição	Exemplo
Nome do país	A abreviação ISO de duas letras para seu país.	US (=Estados Unidos)
Nome do estado ou província	O nome do estado ou província onde sua organização está localizada. Este nome não pode ser abreviado.	Washington
Nome da localidade	A localização de sua organização, como uma cidade.	Seattle
Nome da organização	A razão social completa da sua organização. Não abrevie o nome de sua organização.	Corporação de exemplo
Nome da unidade organizacional	Informações organizacionais adicionais, se houver.	Departamento de exemplo
Nome comum	Esse valor deve corresponder exatamente ao endereço web que você espera que os usuários digitem em um navegador. Geralmente, isso significa um nome de domínio com um nome ou alias de host prefixado na forma <b>www.example.com</b> . Para teste com um certificado autoassinado e nenhuma resolução DNS, o nome comum pode consistir apenas no nome do host. As CAs também oferecem certificados mais caros que aceitam nomes curingas como <b>*.example.com</b> .	www.example.com

Nome	Descrição	Exemplo
Endereço de e-mail	O endereço de e-mail do administrador do servidor.	someone@example.com

Finalmente, a OpenSSL solicita uma senha de desafio opcional. Essa senha se aplica somente à CSR e às transações entre você e sua CA, portanto, siga as recomendações da CA sobre este e o outro campo opcional, nome da empresa opcional. A senha de desafio da CSR não tem nenhum efeito sobre a operação do servidor.

O arquivo resultante **csr.pem** contém sua chave pública, a assinatura digital de sua chave pública e os metadados que você inseriu.

- Envie a CSR a uma CA. Geralmente, isso consiste em abrir seu arquivo de CSR em um editor de texto e copiar o conteúdo em um formulário da Web. Neste momento, pode ser solicitado que você forneça um ou mais nomes alternativos da entidade (SANs) para serem colocados no certificado. Se **www.example.com** for o nome comum, **example.com** seria um bom SAN e vice-versa. Um visitante a seu site que digitar qualquer um desses nomes veria uma conexão livre de erros. Se o formulário da web de sua CA permitir, inclua o nome comum na lista de SANs. Algumas CAs o incluem automaticamente.

Depois que sua solicitação é aprovada, você recebe um novo certificado de host assinado pela CA. Você também pode receber uma instrução para fazer download de um arquivo de certificado intermediário que contém os certificados adicionais necessários para concluir a cadeia de confiança da CA.

#### Note

Sua CA pode enviar a você arquivos em vários formatos com várias finalidades. Para este tutorial, você deve usar apenas um arquivo de certificado em formato PEM que geralmente (mas nem sempre) é identificado por uma extensão **.pem** ou **.crt**. Se você não tiver certeza sobre qual arquivo usar, abra os arquivos com um editor de texto e localize o que contém um ou mais blocos com o seguinte:

```
- - - - -BEGIN CERTIFICATE - - - - -
```

O arquivo também deve terminar com o seguinte:

```
- - - - -END CERTIFICATE - - - - -
```

Você também pode testar um arquivo na linha de comando da seguinte forma:

```
[ec2-user certs]$ openssl x509 -in certificate.crt -text
```

Verifique se as linhas aparecem no arquivo. Não use os arquivos que terminam com **.p7b**, **.p7c** ou extensões de arquivo semelhantes.

- Coloque o novo certificado assinado pela CA e quaisquer certificados intermediários no diretório /etc/pki/tls/certs.

#### Note

Há várias maneiras para fazer upload da chave personalizada para a instância do EC2, mas a maneira mais simples e informativa é abrir um editor de texto (vi, nano, bloco de notas etc.) no seu computador local e na sua instância e, em seguida, copiar e colar os conteúdos do arquivo entre eles. Você precisa de permissões raiz [sudo] ao realizar essas operações na instância do EC2. Dessa forma, você vê imediatamente se há algum problema

de permissão ou de caminho. No entanto, tenha cuidado para não adicionar mais linhas ao copiar o conteúdo ou ao alterá-lo de alguma maneira.

No diretório `/etc/pki/tls/certs`, use os seguintes comandos para verificar se a propriedade do arquivo, o grupo e as configurações de permissão correspondem aos padrões altamente restritivos do Amazon Linux (owner=root, group=root, leitura/gravação somente para o proprietário).

```
[ec2-user certs]$ sudo chown root.root custom.crt
[ec2-user certs]$ sudo chmod 600 custom.crt
[ec2-user certs]$ ls -al custom.crt
```

Os comandos acima devem produzir o seguinte resultado:

```
-rw----- root root custom.crt
```

As permissões para o arquivo de certificado intermediário são menos estritas (owner=root, group=root, proprietário pode gravar, grupo pode ler, mundo pode ler). Os comandos serão:

```
[ec2-user certs]$ sudo chown root.root intermediate.crt
[ec2-user certs]$ sudo chmod 644 intermediate.crt
[ec2-user certs]$ ls -al intermediate.crt
```

Os comandos acima devem produzir o seguinte resultado:

```
-rw-r--r-- root root intermediate.crt
```

6. Se você tiver usado uma chave personalizada para criar sua CSR e o certificado do host resultante, remova ou renomeie a chave antiga no diretório `/etc/pki/tls/private/` e instale a nova chave ali.

#### Note

Há várias maneiras para fazer upload da chave personalizada para a instância do EC2, mas a maneira mais simples e informativa é abrir um editor de texto (vi, nano, bloco de notas etc.) no seu computador local e na sua instância e, em seguida, copiar e colar o conteúdo do arquivo entre eles. Você precisa de privilégios raiz [sudo] ao realizar essas operações na instância do EC2. Dessa forma, você vê imediatamente se há algum problema de permissão ou de caminho. No entanto, tenha cuidado para não adicionar mais linhas ao copiar o conteúdo ou ao alterá-lo de alguma maneira.

Dentro do diretório `/etc/pki/tls/private`, verifique se a propriedade do arquivo, o grupo e as configurações de permissão correspondem aos padrões altamente restritivos do Amazon Linux (owner=root, group=root, leitura/gravação somente para o proprietário). Os comandos seriam os seguintes:

```
[ec2-user private]$ sudo chown root.root custom.key
[ec2-user private]$ sudo chmod 600 custom.key
[ec2-user private]$ ls -al custom.key
```

Os comandos acima devem produzir o seguinte resultado:

```
-rw----- root root custom.key
```

7. Edite `/etc/httpd/conf.d/ssl.conf` para refletir seu novo certificado e arquivos de chave.

- a. Forneça o caminho e o nome do arquivo do certificado de host assinado por CA na diretiva SSLCertificateFile do Apache:

```
SSLCertificateFile /etc/pki/tls/certs/custom.crt
```

- b. Se você receber um arquivo de certificado intermediário (`intermediate.crt` neste exemplo), forneça o caminho e o nome do arquivo usando a diretiva SSLCACertificateFile do Apache:

```
SSLCACertificateFile /etc/pki/tls/certs/intermediate.crt
```

#### Note

Algumas CAs combinam os certificados de host e os certificados intermediários em um único arquivo, o que torna essa diretriz desnecessária. Consulte as instruções fornecidas pela CA.

- c. Forneça o caminho e o nome do arquivo da chave privada na diretiva SSLCertificateKeyFile do Apache.

```
SSLCertificateKeyFile /etc/pki/tls/private/custom.key
```

8. Salve o `/etc/httpd/conf.d/ssl.conf` e reinicie o Apache.

```
[ec2-user ~]$ sudo service httpd restart
```

9. Teste seu servidor inserindo seu nome de domínio em uma barra de URL do navegador com o prefixo `https://`. Seu navegador deve carregar a página de teste via HTTPS sem gerar erros.

## Etapa 3: testar e intensificar a configuração de segurança

Depois que o SSL/TLS estiver operacional e exposto ao público, você precisará testar se ele é realmente seguro. É fácil fazer isso usando serviços online, como o [Qualys SSL Labs](#) que executa uma análise completa e gratuita de sua configuração de segurança. Com base nos resultados, você pode decidir intensificar a configuração de segurança padrão controlando quais protocolos você aceita, quais cifras você prefere e quais você exclui. Para obter mais informações, consulte [como a Qualys formula suas pontuações](#).

#### Important

Os testes no mundo real são cruciais para a segurança do servidor. Pequenos erros de configuração podem resultar em rupturas de segurança sérias e em perda de dados. Como as práticas de segurança recomendadas são alteradas constantemente em resposta a pesquisas e a ameaças emergentes, auditorias periódicas da segurança são essenciais para uma boa administração do servidor.

No site [Qualys SSL Labs](#), digite o nome do domínio totalmente qualificado de seu servidor no formato `www.example.com`. Depois de dois minutos, você recebe uma classificação (de A a F) para seu site e um detalhamento dos resultados. Embora a visão geral mostre que a configuração é mais sólida, o relatório detalhado sinaliza vários problemas possíveis. Por exemplo:

 A codificação RC4 é compatível com o uso por determinados navegadores mais antigos. Uma cifra é o núcleo matemático de um algoritmo de criptografia. A RC4, uma cifra rápida usada para criptografar fluxos de dados TLS, é conhecida por ter várias [fraquezas sérias](#). A menos que você tenha boas razões para oferecer suporte a navegadores legados, você deve desabilitar isso.

X Versões antigas do TLS são compatíveis. A configuração é compatível com o TLS 1.0 (já obsoleto) e o TLS 1.1 (em um caminho para a reprovação). Apenas o TLS 1.2 é recomendado desde 2018.

#### Para corrigir a configuração do TLS

1. Abra o arquivo de configuração /etc/httpd/conf.d/ssl.conf em um editor de texto e comente as seguintes linhas digitando "#" no início de cada uma:

```
#SSLProtocol all -SSLv3  
#SSLProxyProtocol all -SSLv3
```

2. Adicione as seguintes diretivas:

```
SSLProtocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2  
SSLProxyProtocol -SSLv2 -SSLv3 -TLSv1 -TLSv1.1 +TLSv1.2
```

Essas diretivas desativam explicitamente as versões 2 e 3 do SSL, bem como as versões 1.0 e 1.1 do TLS. O servidor agora se recusa a aceitar conexões criptografadas com clientes que não estejam usando o TLS 1.2. A expressão detalhada na diretriz comunica mais claramente, para um leitor humano, para que o servidor está configurado.

#### Note

Desabilitar as versões 1.0 e 1.1 do TLS dessa forma bloqueia o acesso ao seu site de uma pequena porcentagem de navegadores da web desatualizados.

#### Para modificar a lista de cifras permitidas

1. Abra o arquivo de configuração /etc/httpd/conf.d/ssl.conf localize a seção com exemplos comentados para a configuração de **SSLCipherSuite** e **SSLProxyCipherSuite**.

```
#SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5  
#SSLProxyCipherSuite HIGH:MEDIUM:!aNULL:!MD5
```

Deixe-os como estão e, abaixo deles, adicione as seguintes diretrizes:

#### Note

Embora sejam mostradas em várias linhas aqui para facilitar a leitura, cada uma dessas diretrizes deve estar em uma única linha sem espaços entre os nomes das cifras.

```
SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-  
CHACHA20-POLY1305:  
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-  
SHA256:ECDHE-ECDSA-AES256-SHA384:  
ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES:!aNULL:  
eNULL:!EXPORT:!DES:  
!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA  
  
SSLProxyCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-  
ECDSA-CHACHA20-POLY1305:  
ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-  
SHA256:ECDHE-ECDSA-AES256-SHA384:  
ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:AES:!aNULL:  
eNULL:!EXPORT:!DES:  
!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA
```

Essas cifras são um subconjunto da lista muito mais longa de cifras com suporte na OpenSSL. Foram selecionadas e ordenadas de acordo com os seguintes critérios:

- Suporte para forward secrecy
- Força
- Velocidade
- Cifras específicas antes das famílias de cifras
- Cifras permitidas antes das cifras negadas

As cifras com classificações elevadas têm ECDHE nos seus nomes, para Elliptic Curve Diffie-Hellman Ephemeral (Curva elíptica de Diffie-Hellman efêmera); o termo efêmera indica o forward secrecy (sigilo de encaminhamento). Além disso, a RC4 agora está entre as cifras proibidas no final.

Recomendamos que você use uma lista explícita de cifras em vez de confiar em padrões ou em diretrizes concisas cujo conteúdo não é visível. A lista de cifras mostrada aqui é apenas uma das muitas listas possíveis. Por exemplo, você pode desejar otimizar uma lista para velocidade em vez de forward secrecy.

Se você antecipar uma necessidade de oferecer suporte a clientes mais antigos, você pode habilitar o pacote de cifras DES-CBC3-SHA.

Cada atualização do OpenSSL introduz novas cifras e torna obsoletas as cifras antigas. Mantenha sua instância do EC2 do Amazon Linux atualizada e fique atento às notificações de segurança do [OpenSSL](#) e às notícias sobre novas descobertas em segurança na imprensa técnica.

2. Exclua o comentário da linha a seguir removendo o "#":

```
#SSLHonorCipherOrder on
```

Esse comando força o servidor a preferir cifras de alta classificação incluindo (neste caso) aquelas que oferecem suporte a forward secrecy. Com essa diretriz ativada, o servidor tenta estabelecer uma conexão altamente segura antes de voltar a usar cifras permitidas com menos segurança.

3. Reinicie o Apache. Se você testar o domínio novamente no [Qualys SSL Labs](#), verá que a vulnerabilidade do RC4 desapareceu.

## Troubleshoot

- Meu servidor da web do Apache não será iniciado, a menos que eu digite uma senha

Esse é comportamento esperado se você tiver instalado uma chave privada de servidor criptografada e protegida por senha.

Você pode remover a criptografia e a solicitação de senha da chave. Supondo que você tenha uma chave de RSA privada criptografada chamada `custom.key` no diretório padrão, e que a senha seja `abcde12345`, execute os comandos a seguir na sua instância do EC2 para gerar uma versão descriptografada da chave:

```
[ec2-user ~]$ cd /etc/pki/tls/private/  
[ec2-user private]$ sudo cp custom.key custom.key.bak  
[ec2-user private]$ sudo openssl rsa -in custom.key -passin pass:abcde12345 -out  
    custom.key.nocrypt  
[ec2-user private]$ sudo mv custom.key.nocrypt custom.key  
[ec2-user private]$ sudo chown root.root custom.key  
[ec2-user private]$ sudo chmod 600 custom.key
```

```
[ec2-user private]$ sudo service httpd restart
```

O Apache agora deve iniciar sem solicitar uma senha a você.

# 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.

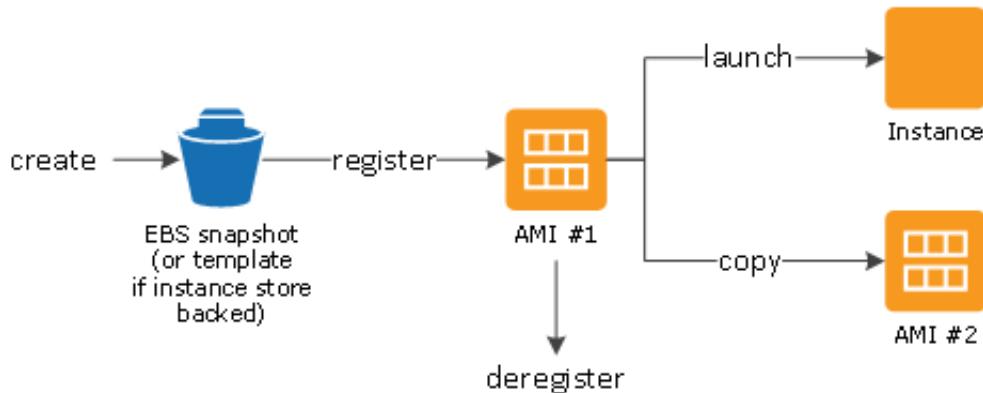
## Tópicos

- [Usar uma AMI \(p. 72\)](#)
- [Criar sua própria AMI \(p. 73\)](#)
- [Comprar, compartilhar e vender AMIs \(p. 73\)](#)
- [Cancelar o registro da AMI \(p. 74\)](#)
- [Amazon Linux 2 e Amazon Linux AMI \(p. 74\)](#)
- [Tipos de AMI \(p. 74\)](#)
- [Tipos de virtualização da AMI em Linux \(p. 77\)](#)
- [Modos de inicialização \(p. 79\)](#)
- [Localizar uma AMI do Linux \(p. 87\)](#)
- [AMIs compartilhadas \(p. 92\)](#)
- [AMIs pagas \(p. 102\)](#)
- [Ciclo de vida da AMI \(p. 106\)](#)
- [Usar criptografia com AMIs com EBS \(p. 163\)](#)
- [Noções básicas sobre as informações de faturamento da AMI \(p. 168\)](#)
- [Amazon Linux \(p. 172\)](#)
- [Kernels fornecidos pelo usuário \(p. 191\)](#)
- [Configure a conexão de desktop MATE Amazon Linux 2 \(p. 197\)](#)

## Usar uma AMI

O diagrama a seguir resume o ciclo de vida da AMI. Após criar e registrar uma AMI, você pode usá-la para executar novas instâncias. (Você também pode executar instâncias em uma AMI se o proprietário da AMI

conceder permissões de execução a você.) Você pode copiar uma AMI dentro da mesma AWS região ou para regiões da AWS diferentes. Quando não precisar mais de uma AMI, você poderá cancelar o registro dela.



Você pode pesquisar uma AMI que atenda aos critérios para sua instância. Você pode pesquisar AMIs fornecidas pela AWS ou AMIs fornecidas pela comunidade. Para obter mais informações, consulte [Tipos de AMI \(p. 74\)](#) e [Localizar uma AMI do Linux \(p. 87\)](#).

Depois de iniciar uma instância em uma AMI, você pode se conectar a ela. Quando você está conectado a uma instância, você pode usá-la da mesma forma como usa outro servidor. Para obter informações sobre a execução, a conexão e o uso de sua instância, consulte [Tutorial: Comece a usar instâncias Linux do Amazon EC2 \(p. 9\)](#).

## Criar sua própria AMI

Por exemplo, você pode executar uma instância com base em uma AMI existente, personalizar a instância do (por exemplo, [instalar software \(p. 600\)](#) na instância) e, em seguida, salvar esta configuração atualizada como uma AMI personalizada. Entre as instâncias executadas nessa AMI personalizada estão as personalizações que você fez quando criou a AMI.

O dispositivo de armazenamento raiz da instância determina o processo que você segue para criar uma AMI. O volume raiz de uma instância é um volume do Amazon Elastic Block Store (Amazon EBS) ou um volume de armazenamento de instâncias. Para obter mais informações sobre volumes de dispositivos raiz, consulte [Volume do dispositivo raiz da instância do Amazon EC2 \(p. 1521\)](#).

- Para criar uma AMI com Amazon EBS, consulte [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#).
- Para criar uma AMI com armazenamento de instâncias, consulte [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#).

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 \(p. 1552\)](#).

## Comprar, compartilhar e vender AMIs

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 \(p. 92\)](#).

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. Para obter mais informações sobre como comprar ou vender AMIs, consulte [AMIs pagas \(p. 102\)](#).

## Cancelar o registro da AMI

Você pode cancelar o registro de uma AMI, quando não precisar mais dela. Depois de cancelar o registro de uma AMI, ela não poderá ser usada para executar novas instâncias. As instâncias existentes executadas na AMI não são afetadas. Para obter mais informações, consulte [Cancelar AMI do Linux \(p. 159\)](#).

## Amazon Linux 2 e Amazon Linux AMI

O Amazon Linux 2 e o Amazon Linux AMI são compatíveis e mantidos nas imagens do Linux fornecidas pela AWS. A seguir encontram-se alguns dos recursos do Amazon Linux 2 e do Amazon Linux AMI:

- Um ambiente de execução estável, seguro e de alta performance para aplicações em execução no Amazon EC2.
- Fornecido gratuitamente aos usuários do Amazon EC2.
- Acesso ao repositório para várias versões do MySQL, PostgreSQL, Python, Ruby, Tomcat e de muitos outros pacotes comuns.
- Atualizado regularmente para incluir os componentes mais recentes. Essas atualizações também são disponibilizadas nos repositórios yum para instalação em instâncias em execução.
- Inclui pacotes que permitem integração fácil com os produtos da AWS, como a AWS CLI, a API do Amazon EC2 e as ferramentas de AMI, a biblioteca Boto para Python e as ferramentas do Elastic Load Balancing.

Para obter mais informações, consulte [Amazon Linux \(p. 172\)](#).

## Tipos de AMI

Você pode selecionar uma AMI para uso com base nas seguintes características:

- Região (consulte [Regiões e zonas \(p. 923\)](#))
- Sistema operacional
- Arquitetura (32 bits ou 64 bits)
- [Permissões de execução \(p. 74\)](#)
- [Armazenamento para o dispositivo raiz \(p. 75\)](#)

## Permissões de execução

O proprietário de uma AMI determina sua disponibilidade especificando permissões de execução. As permissões de execução entram nas seguintes categorias.

Permissão de execução	Descrição
pública	O proprietário concede permissões de execução a todas as contas da AWS.
explícita	O proprietário concede permissões de execução a contas específicas da AWS.
implícita	O proprietário tem permissões de execução implícitas para uma AMI.

A Amazon e a comunidade do Amazon EC2 fornecem uma grande seleção de AMIs públicas. Para obter mais informações, consulte [AMIs compartilhadas \(p. 92\)](#). Os desenvolvedores podem cobrar por suas AMIs. Para obter mais informações, consulte [AMIs pagas \(p. 102\)](#).

## Armazenamento para o dispositivo raiz

Todas as AMIs são categorizadas como com Amazon EBS ou com armazenamento de instâncias. A primeira significa que o dispositivo raiz de uma instância executada na AMI é um volume do Amazon Elastic Block Store (Amazon EBS) criado em um snapshot do Amazon EBS. A última significa que o dispositivo raiz de uma instância executada na AMI é um volume de armazenamento de instâncias criado em um modelo no Amazon S3. Para obter mais informações, consulte [Volume do dispositivo raiz da instância do Amazon EC2 \(p. 1521\)](#).

A tabela a seguir resume as diferenças importantes ao usar os dois tipos de AMIs.

Característica	AMI com Amazon EBS	AMI com armazenamento de instâncias da Amazon
Tempo de inicialização para uma instância	Geralmente menos que 1 minuto	Geralmente menos que 5 minutos
Limite de tamanho para um dispositivo raiz	64 TiB	10 GiB
Volume do dispositivo raiz	Volume do EBS	Volumes de armazenamento de instâncias
Persistência de dados	Por padrão, o volume raiz é excluído quando a instância é encerrada.* Os dados em todos os outros volumes do EBS persistem após o encerramento da instância, por padrão.	Os dados em qualquer volume do armazenamento de instâncias persistem apenas durante a vida útil da instância.
Modificações	O tipo de instância, o kernel, o disco da RAM e os dados do usuário podem ser alterados enquanto a instância está parada.	Os atributos de instância são fixos durante a vida útil de uma instância.
Cobranças	Você é cobrado pelo uso de instância, uso de volume do EBS; e pelo armazenamento da AMI como um snapshot do EBS.	Você é cobrado pelo uso da instância e pelo armazenamento da AMI no Amazon S3.
Criação/empacotamento da AMI	Usa um único comando/chamada	Requer instalação e uso de ferramentas de AMI

Característica	AMI com Amazon EBS	AMI com armazenamento de instâncias da Amazon
Estado parado	Pode estar em um estado interrompido. Mesmo quando a instância é interrompida e não está em execução, o volume raiz permanece no Amazon EBS	Não pode estar no estado parado. As instâncias estão em execução ou encerradas

\* Por padrão, os volumes raiz do EBS têm o sinalizador `DeleteOnTermination` definido como `true`. Para obter informações sobre como alterar esse sinalizador para que o volume persista depois do encerramento, consulte [Alterar o volume raiz para persistir \(p. 1525\)](#).

\*\* Compatível apenas com `io2` EBS Block Express. Para obter mais informações, consulte [Volumes `io2` do Block Express \(p. 1262\)](#).

## Determinar o tipo de dispositivo raiz da AMI

Para determinar o tipo de dispositivo raiz de uma AMI usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, clique em AMIs e selecione a AMI.
3. Verifique o valor de Root Device Type (Tipo de dispositivo raiz) na guia Details (Detalhes) da seguinte maneira:
  - Se o valor é `ebs`, esta é uma AMI com Amazon EBS.
  - Se o valor for `instance store`, esta será uma AMI com armazenamento de instâncias.

Para determinar o tipo de dispositivo raiz de 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 \(p. 3\)](#).

- [describe-images](#) (AWS CLI)
- [Get-EC2Image](#) (AWS Tools for Windows PowerShell)

## Estado parado

Você pode interromper uma instância com Amazon EBS, mas não uma instância com armazenamento de instâncias do Amazon EC2. Parar faz com que a instância pare de executar (seu status muda de `running` para `stopping` e para `stopped`). Uma instância parada persiste no Amazon EBS, o que permite que ela seja reiniciada. Parar é diferente de encerrar. Você não pode reiniciar uma instância encerrada. Como as instâncias com suporte do armazenamento de instâncias do Amazon EC2 não podem ser paradas, elas estão em execução ou encerradas. Para obter mais informações sobre o que acontece e o que você pode fazer enquanto uma instância está parada, consulte [Interromper e iniciar sua instância \(p. 562\)](#).

## Persistência e armazenamento de dados padrão

As instâncias que usam um volume de armazenamento de instâncias para o dispositivo raiz automaticamente têm armazenamento de instâncias disponível (o volume raiz contém a partição raiz, e você pode armazenar dados adicionais). Você pode adicionar armazenamento persistente à instância anexando um ou mais volumes do EBS. Todos os dados em um volume de armazenamento de instâncias são excluídos quando a instância falha ou é encerrada. Para obter mais informações, consulte [Vida útil do armazenamento de instâncias \(p. 1495\)](#).

As instâncias que usam o Amazon EBS para dispositivo raiz automaticamente têm um volume do EBS associado. O volume aparece em sua lista de volumes como qualquer outro. Com a maioria dos tipos de instância, por padrão, as instâncias com suporte do Amazon EBS não têm volumes de armazenamento de instâncias. Você pode adicionar volumes de armazenamento de instâncias ou volumes do EBS adicionais usando um mapeamento de dispositivos de blocos. Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1530\)](#).

## Tempos de inicialização

As instâncias executadas a partir de uma AMI baseada em Amazon EBS são executadas mais rapidamente do que as instâncias executadas a partir de uma AMI com armazenamento de instâncias. Quando você executa uma instância a partir de um AMI com armazenamento de instâncias, todas as partes precisam ser recuperadas do Amazon S3 para que a instância fique disponível. Com uma AMI com suporte do Amazon EBS, apenas as partes necessárias para inicializar a instância precisam ser recuperadas do snapshot para que a instância fique disponível. Contudo, a performance de uma instância que usa um volume do EBS para seu dispositivo raiz é mais lento por um breve período enquanto as partes restantes são recuperadas do snapshot e carregadas no volume. Quando você para e reinicia a instância, ela é executada rapidamente, porque o estado é armazenado em um volume do EBS.

## Criação de AMIs

Para criar AMIs do Linux com armazenamento de instâncias, você deve criar uma AMI de sua instância na própria instância usando as ferramentas de AMI do Amazon EC2.

A criação de AMIs é muito mais fácil para AMIs com suporte do Amazon EBS. A ação da API `CreateImage` cria a AMI com Amazon EBS e a registra. Há também um botão no AWS Management Console que permite criar uma AMI em uma instância em execução. Para obter mais informações, consulte [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#).

## Como você é cobrado

Com as AMIs com suporte do armazenamento de instâncias, você é cobrado pelo uso da instância e para armazenar a AMI no Amazon S3. Com as AMIs com suporte de Amazon EBS, você é cobrado pelo uso da instância, pelo uso e armazenamento de volume do EBS; e por armazenar a AMI como um snapshot do EBS.

Nas AMIs com armazenamento de instâncias do Amazon EC2, toda vez que você personaliza uma AMI e cria uma nova, todas as partes são armazenadas no Amazon S3 para cada AMI. Portanto, o volume de armazenamento de cada AMI personalizada é o tamanho completo da AMI. Para AMIs com suporte do Amazon EBS, sempre que você personaliza uma AMI e cria um nova, apenas as alterações são armazenadas. Portanto, o volume do armazenamento para AMIs subsequentes que você personaliza depois da primeira é muito menor resultando em cobranças menores de armazenamento de AMI.

Quando uma instância com suporte do Amazon EBS é parada, você não é cobrado pelo uso da instância. No entanto, você ainda é cobrado pelo armazenamento de volume. Assim que você iniciar a sua instância, cobraremos por um mínimo de um minuto por 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. Nós cobramos por cada segundo, com um mínimo de um minuto, que você mantenha a instância em execução, mesmo que a instância permaneça ociosa e você não se conecte a ela.

## Tipos de virtualização da AMI em Linux

As Imagens de máquina da Amazon em Linux usam um dos dois tipos de virtualização: 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 (CPU, rede e armazenamento) para melhor performance.

Para melhor performance, recomendamos que você use os tipos de instância da geração atual e AMIs HVM quando executar suas instâncias. Para obter mais informações sobre os tipos de instâncias da atual geração, consulte [Tipos de instância do Amazon EC2](#). Se você estiver usando tipos de instância da geração anterior e quiser fazer uma atualização, consulte [Caminhos de atualização](#).

A tabela a seguir compara AMIs de HVM e PV.

	HVM	PV
Descrição	<p>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.</p>	<p>As AMIs PV são inicializadas com um bootloader especial chamado PV-GRUB, que começa o ciclo de inicialização e encadeia e carrega o kernel especificado no arquivo menu.lst da sua imagem. Os convidados paravirtuais podem ser executados em hardware de host que não é explicitamente compatível para virtualização. Historicamente, os guests PV têm melhor performance que os guests HVM em muitos casos, mas devido a aprimoramentos na virtualização de HVM e disponibilidade de drivers PV para AMIs HVM, isso não é mais verdadeiro. Para obter mais informações sobre o PV-GRUB e seu uso no Amazon EC2, consulte <a href="#">Enabling Your Own Linux Kernels (p. 191)</a>.</p>
Suporte para extensões de hardware	<p>Sim. Ao contrário de guests PV, os guests HVM podem aproveitar as extensões de hardware que fornecem acesso rápido ao hardware subjacente no sistema host. Para obter mais informações quanto às extensões de virtualização da CPU disponíveis no Amazon EC2, consulte <a href="#">Intel Virtualization Technology</a>, no site da Intel. 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. Para obter mais</p>	<p>Não, eles não podem beneficiar-se de extensões de hardware especiais, como rede avançada ou processamento de GPU.</p>

	HVM	PV
	informações, consulte <a href="#">Rede avançada no Linux (p. 1015)</a> e <a href="#">Linux Instâncias computacionais aceleradas do (p. 305)</a> .	
Tipos de instâncias compatíveis	Todos os tipos de instância da geração atual são compatíveis com AMIs HVM.	Os seguintes tipos de instância da geração anterior são compatíveis com AMIs PV: C1, C3, HS1, M1, M3, M2 e T1. Os tipos de instância da geração atual não são compatíveis com AMIs PV.
Regiões compatíveis	Todas as regiões são compatíveis com instâncias HVM.	Ásia-Pacífico (Tóquio), Ásia-Pacífico (Cingapura), Ásia-Pacífico (Sydney), Europa (Frankfurt), Europa (Irlanda), América do Sul (São Paulo), US East (N. Virginia), Oeste dos EUA (Norte da Califórnia) e Oeste dos EUA (Oregon)
Como encontrar	Verifique se o tipo de virtualização da AMI está definido como <code>hvm</code> usando o console ou o comando <a href="#">describe-images</a> .	Verifique se o tipo de virtualização da AMI está definido como <code>paravirtual</code> usando o console ou o comando <a href="#">describe-images</a> .

#### PV em HVM

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, esses drivers PV estão disponíveis para guests HVM, de forma que os sistemas operacionais que não puderem ser movidos para execução em um ambiente paravirtualizado ainda poderão ver 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, ou melhor, que os guests paravirtuais.

## 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 \(p. 80\)](#)
- [Requisitos para executar uma instância com UEFI \(p. 80\)](#)
- [Determinar o parâmetro de modo de inicialização de uma AMI \(p. 81\)](#)
- [Determinar os modos de inicialização suportados por um tipo de instância \(p. 82\)](#)
- [Determinar o modo de inicialização de uma instância \(p. 82\)](#)
- [Determinar o modo de inicialização do sistema operacional \(p. 83\)](#)
- [Definir o modo de inicialização de uma AMI \(p. 84\)](#)

## 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 \(p. 82\)](#).
- 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 \(p. 83\)](#).

- 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 \(p. 81\)](#).

A AWS não fornece AMIs previamente configuradas para oferecer suporte a UEFI. É necessário [configurar a AMI \(p. 84\)](#), 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 \(AMI\) \(p. 511\)](#).

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 SSH.

Para determinar o modo de inicialização do sistema operacional da instância

1. [Conecte-se à instância do Linux usando SSH \(p. 538\)](#).
2. Para visualizar o modo de inicialização do sistema operacional, tente um dos seguintes procedimentos:
  - Execute o seguinte comando.

```
[ec2-user ~]$ sudo /usr/sbin/efibootmgr
```

Saída esperada de uma instância inicializada no modo de inicialização UEFI

```
BootCurrent: 0001
Timeout: 0 seconds
BootOrder: 0000,0001,0002
Boot0000* UiaApp
Boot0001* UEFI Amazon Elastic Block Store vol-xyz
Boot0002* EFI Internal Shell
```

- Execute o seguinte comando para verificar a existência do diretório `/sys/firmware/efi`. Esse diretório só existirá se a instância for inicializada usando UEFI. Se o diretório não existir, o comando retornará `Legacy BIOS Boot Detected`.

```
[ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo "Legacy
BIOS Boot Detected"
```

Saída esperada de uma instância inicializada no modo de inicialização UEFI

```
UEFI Boot Detected
```

Saída esperada de uma instância inicializada no modo de inicialização BIOS legado

```
Legacy BIOS Boot Detected
```

- Execute o seguinte comando para verificar se EFI aparece na saída `dmesg`.

```
[ec2-user ~]$ dmesg | grep -i "EFI"
```

Saída esperada de uma instância inicializada no modo de inicialização UEFI

```
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: EFI v2.70 by EDK II
```

## 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. 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,  
            "VolumeId": "vol-049df61146c4d7901",  
            "State": "completed",  
            "VolumeSize": 8,  
            "StartTime": "2019-02-28T21:28:32.000Z",  
            "Progress": "100%",  
            "OwnerId": "012345678910",  
            "SnapshotId": "snap-01234567890abcdef",  
            ...  
    ]  
}
```

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](#).

## Localizar uma AMI do Linux

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`), 64 bits (`x86_64`) ou ARM de 64 bits (`arm64`)
- O tipo de dispositivo raiz: Amazon EBS ou armazenamento de instâncias
- O provedor (por exemplo, Amazon Web Services)
- Software adicional (por exemplo, SQL Server)

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

### Tópicos

- [Localizar uma AMI do Linux usando o console do Amazon EC2 \(p. 87\)](#)
- [Localizar uma AMI usando o AWS CLI \(p. 88\)](#)
- [Localizar a AMI do Amazon Linux mais recente usando o Systems Manager \(p. 88\)](#)
- [Use um parâmetro de Systems Manager para localizar uma AMI \(p. 89\)](#)

## Localizar uma AMI do Linux usando o console do Amazon EC2

Você pode encontrar AMIs do Linux 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 Linux 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 \(AMI\) \(p. 511\)](#).

### Para localizar uma AMI do Linux 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 Linux 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. Antes de selecionar uma AMI, é importante que você verifique se ela é baseada em um armazenamento de instâncias ou no Amazon EBS e se você está ciente dos efeitos dessa diferença. Para obter mais informações, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#).
7. 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 \(p. 512\)](#). Se você não estiver pronto para executar a instância agora, anote o ID da AMI para consultar depois.

## Localizar uma AMI usando o AWS CLI

Você pode usar comandos da AWS CLI do Amazon EC2 para listar somente as AMIs do Linux 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).

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 compatíveis com o Amazon EBS:

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

### Important

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

## Localizar a AMI do Amazon Linux 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. Por exemplo, o parâmetro `/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2` fornecido pelo EC2 está disponível em todas as regiões e sempre aponta para a versão mais recente da AMI do Amazon Linux 2 em uma região.

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

---

/aws/service/ami-amazon-linux-latest

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

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

Como executar uma instância usando um parâmetro público

O exemplo a seguir usa o parâmetro público fornecido pelo EC2 para executar uma instância `m5.xlarge` usando a AMI do Amazon Linux 2 mais recente.

Para especificar o parâmetro no comando, use a seguinte sintaxe: `resolve:ssm:public-parameter`, onde `resolve:ssm` é o prefixo padrão e `public-parameter` é o caminho e o nome do parâmetro público.

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:/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2  
  --instance-type m5.xlarge  
  --key-name MyKeyPair
```

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 Amazon Linux AMI IDs Using AWS Systems Manager Parameter Store](#) (Consultar os IDs de AMI do Amazon Linux mais recentes 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 \(p. 90\)](#)
- [Executar uma instância usando um parâmetro de Systems Manager \(p. 90\)](#)
- [Permissions \(p. 91\)](#)
- [Limitations \(p. 92\)](#)

## 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 selecionem um parâmetro do Systems Manager para localizar a AMI. Ao exigir que os usuários selecionem 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 selecionem 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 Linux 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 \(AMI\) \(p. 511\)](#).

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 do Linux baseada em armazenamento em instância](#) ou [Criação de uma AMI do Linux baseada no Amazon EBS](#). Para obter informações sobre como criar, fornecer e manter suas aplicações no AWS Marketplace , consulte a [Documentação do AWS Marketplace](#) .

### Tópicos

- [Encontrar AMIs compartilhadas \(p. 92\)](#)
- [Tornar um AMI pública \(p. 95\)](#)
- [Compartilhar uma AMI com contas específicas da AWS \(p. 96\)](#)
- [Usar marcadores \(p. 97\)](#)
- [Diretrizes para AMIs em Linux compartilhadas \(p. 98\)](#)

## 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 \(p. 144\)](#).

### Tópicos

- [Encontrar uma AMI compartilhada \(console\) \(p. 93\)](#)
- [Localizar uma AMI compartilhada \(AWS CLI\) \(p. 93\)](#)
- [Usar AMIs compartilhadas \(p. 94\)](#)

## 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 (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"
```

## Usar AMIs compartilhadas

Para que você use uma AMI compartilhada, execute as etapas a seguir para confirmar se não há credenciais pré-instaladas que permitam acesso indesejado à sua instância por terceiros e nenhum registro remoto pré-configurado que poderia transmitir dados confidenciais a terceiros. Verifique documentação da distribuição Linux usada pelas informações da AMI para obter informações sobre melhora da segurança do sistema.

Para garantir que você não perca accidentalmente acesso à sua instância, recomendamos que inicie duas sessões de SSH e mantenha a segunda sessão aberta até remover as credenciais que não reconhece e ter confirmado que ainda pode fazer login em sua instância usando SSH.

1. Identifique e desabilite todas as chaves SSH públicas não autorizadas. A única chave no arquivo deve ser aquela usada para executar as AMIs. O seguinte comando localiza os arquivos `authorized_keys`:

```
[ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
```

2. Desabilita a autenticação baseada em senha para o usuário raiz. Abra o arquivo `sshd_config` e edite a linha `PermitRootLogin` da seguinte forma:

```
PermitRootLogin without-password
```

Como alternativa, você pode desativar a capacidade de fazer login na instância como usuário raiz:

```
PermitRootLogin No
```

Reinicie o serviço sshd.

3. Verifique se há alguma outra conta de usuário que possa fazer login na sua instância. Contas com privilégios de superusuário são particularmente perigosas. Remova ou bloqueeie senha de todas as contas desconhecidas.
4. Verifique se há portas abertas que você não está usando e escuta de serviços de rede em execução para as conexões de entrada.
5. Para evitar o registro em log remoto pré-configurado, exclua o arquivo de configuração existente e reinicie o serviço rsyslog. Por exemplo:

```
[ec2-user ~]$ sudo rm /etc/rsyslog.conf
[ec2-user ~]$ sudo service rsyslog restart
```

6. Verifique se todos os trabalhos cron são legítimos.

Se você descobrir uma AMI pública que sente que apresenta um risco de segurança, entre em contato com a equipe de segurança da AWS. Para obter informações, consulte o [Centro de segurança da AWS](#).

## 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 \(p. 96\)](#)). 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 \(p. 144\)](#).

Para evitar expor dados confidenciais ao compartilhar uma AMI, leia as considerações de segurança em [Diretrizes para AMIs em Linux compartilhadas \(p. 98\)](#) e siga as ações recomendadas.

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 \(console\) \(p. 95\)](#)
- [Compartilhar uma AMI com todas as contas da AWS \(AWS CLI\) \(p. 95\)](#)

## 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 (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 `a11`. 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 `a11` 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 \(p. 1319\)](#). 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 \(p. 144\)](#).

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 \(p. 1319\)](#).

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 \(p. 92\)](#).

## 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 \(p. 1319\)](#).

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.

## Diretrizes para AMIs em Linux compartilhadas

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

### Important

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.

#### Tópicos

- [Atualização das ferramentas de AMI antes do uso \(p. 99\)](#)
- [Desabilitar logins remotos com senha para raiz \(p. 99\)](#)
- [Desabilitar o acesso à raiz local \(p. 99\)](#)
- [Remover pares de chave do host SSH \(p. 99\)](#)
- [Instalação de credenciais de chave pública \(p. 100\)](#)
- [Desabilitar as verificações DNS sshd \(opcional\) \(p. 101\)](#)
- [Identifique-se \(p. 102\)](#)
- [Proteja-se \(p. 102\)](#)

Se você estiver criando AMIs para AWS Marketplace , consulte [Best practices for building AMIs](#) (Práticas recomendadas para criar AMIs) no [AWS Marketplace Seller Guide](#) (Guia para vendedores do AWS Marketplace) para obter diretrizes, políticas e práticas recomendadas.

Para obter informações adicionais sobre compartilhamento de AMIs com segurança, consulte os seguintes artigos:

- [Como compartilhar e usar AMIs públicas de forma segura](#)
- [Public AMI Publishing: Hardening and Clean-up Requirements](#)

## Atualização das ferramentas de AMI antes do uso

Para AMIs com armazenamento de instâncias, recomendamos que suas AMIs façam download e atualizem as ferramentas de criação de AMI do Amazon EC2 antes de usá-las. Isso garante que as novas AMIs baseadas nas suas AMIs compartilhadas tenham as ferramentas de AMI mais recentes.

No [Amazon Linux 2](#), instale o pacote `aws-amitools-ec2` e adicione as ferramentas de AMI no seu caminho com o comando a seguir. No [Amazon Linux AMI](#), o pacote `aws-amitools-ec2` já vem instalado por padrão.

```
[ec2-user ~]$ sudo yum install -y aws-amitools-ec2 && export PATH=$PATH:/opt/aws/bin > /etc/profile.d/aws-amitools-ec2.sh && . /etc/profile.d/aws-amitools-ec2.sh
```

Atualize as ferramentas de AMI com o comando a seguir:

```
[ec2-user ~]$ sudo yum upgrade -y aws-amitools-ec2
```

Para outras distribuições, tenha as ferramentas de AMI mais recentes.

## Desabilitar logins remotos com senha para raiz

Usar uma senha de raiz fixa com uma AMI pública é um risco de segurança que pode rapidamente ficar conhecido. Até mesmo depender dos usuários para alterar a senha depois do primeiro login abre uma pequena janela de oportunidade para potencial abuso.

Para resolver esse problema, desabilite logins remotos com senha para o usuário raiz.

Para desabilitar logins remotos com senha para raiz

1. Abra o arquivo `/etc/ssh/sshd_config` com um editor de texto e localize a seguinte linha:

```
#PermitRootLogin yes
```

2. Altere a linha para:

```
PermitRootLogin without-password
```

O local desse arquivo de configuração pode diferir para sua distribuição ou se você não estiver executando OpenSSH. Se esse for o caso, consulte a documentação apropriada.

## Desabilitar o acesso à raiz local

Quando você trabalha com AMIs compartilhadas, a prática recomendada é desabilitar logins diretos na raiz. Para isso, faça login na sua instância em execução e emita o seguinte comando:

```
[ec2-user ~]$ sudo passwd -l root
```

Note

Esse comando não afeta o uso de `sudo`.

## Remover pares de chave do host SSH

Se você pretende compartilhar uma AMI derivada de uma AMI pública, remova os pares de chaves do host SSH existentes localizadas em `/etc/ssh`. Isso força o SSH a gerar novos pares de chaves SSH

exclusivos quando alguém executar uma instância usando sua AMI, melhorando a segurança e reduzindo a probabilidade de ataques "man-in-the-middle".

Elimine todos os arquivos de chave a seguir presentes no seu sistema.

- `ssh_host_dsa_key`
- `ssh_host_dsa_key.pub`
- `ssh_host_key`
- `ssh_host_key.pub`
- `ssh_host_rsa_key`
- `ssh_host_rsa_key.pub`
- `ssh_host_ecdsa_key`
- `ssh_host_ecdsa_key.pub`
- `ssh_host_ed25519_key`
- `ssh_host_ed25519_key.pub`

Você pode remover com segurança todos esses arquivos com o comando a seguir.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

#### Warning

Utilitários de exclusão segura, como `shred`, podem não remover todas as cópias de um arquivo da sua mídia de armazenamento. Podem ser criadas cópias ocultas de arquivos ao criar registros dos sistemas de arquivos (incluindo Amazon Linux padrão ext4), snapshots, backups, RAID e cache temporário. Para obter mais informações, consulte a [documentação](#) do `shred`.

#### Important

Se você se esquecer de remover o par de chaves existente do host SSH da AMI pública, nosso processo de auditoria de rotina notificará você e todos os clientes que executam instâncias da sua AMI sobre o risco potencial à segurança. Após um breve período de carência, marcamos a AMI como privada.

## Instalação de credenciais de chave pública

Depois de configurar a AMI para impedir o login usando uma senha, você deve garantir que os usuários possam fazer login usando outro mecanismo.

O Amazon EC2 permite que os usuários especifiquem um nome de par de chaves público-privado ao executarem uma instância. Quando um nome válido de par de chaves for fornecido para a chamada de API `RunInstances` (ou pelas ferramentas de API da linha de comando), a chave pública (a parte do par de chaves que o Amazon EC2 retém no servidor depois de uma chamada para `CreateKeyPair` ou `ImportKeyPair`) será disponibilizada para a instância por meio de uma consulta HTTP contra os metadados de instância.

Para fazer login com SSH, sua AMI deve recuperar o valor da chave na inicialização e anexá-la a `/root/.ssh/authorized_keys` (ou o equivalente para qualquer outra conta de usuário na AMI). Os usuários podem executar instâncias da sua AMI com um par de chaves e fazer login sem exigir uma senha raiz.

Muitas distribuições, inclusive Amazon Linux e Ubuntu, usam o pacote `cloud-init` para injetar credenciais de chave pública a um usuário configurado. Se sua distribuição não oferecer suporte a

cloud-init, você pode adicionar o código a seguir a um script de inicialização do sistema (como `/etc/rc.local`) para puxar a chave pública especificada na execução para o usuário raiz.

**Note**

No exemplo a seguir, o endereço IP do `http://169.254.169.254/` é um endereço local de link e é válido apenas a partir da instância.

**IMDSv2**

```
if [ ! -d /root/.ssh ] ; then
    mkdir -p /root/.ssh
    chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
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/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
    cat /tmp/my-key >> /root/.ssh/authorized_keys
    chmod 700 /root/.ssh/authorized_keys
    rm /tmp/my-key
fi
```

**IMDSv1**

```
if [ ! -d /root/.ssh ] ; then
    mkdir -p /root/.ssh
    chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
    cat /tmp/my-key >> /root/.ssh/authorized_keys
    chmod 700 /root/.ssh/authorized_keys
    rm /tmp/my-key
fi
```

Isso pode ser aplicado a qualquer conta de usuário; você não precisa restringir a `root`.

**Note**

Reempacotar uma instância baseada nessa AMI inclui a chave com a qual ela foi executada. Para evitar a inclusão de chaves, você deve desmarcar (ou excluir) o arquivo `authorized_keys` ou excluir esse arquivo do reempacotamento.

## Desabilitar as verificações DNS sshd (opcional)

Desabilitar as verificações de DNS sshd enfraquece levemente a segurança de sshd. Contudo, se uma solução de DNS falhar, o login de SSH continuará funcionando. Se você não desabilitar verificações de sshd, falhas de resolução de DNS impedirão todos os logins.

Para desabilitar as verificações de DNS sshd

1. Abra o arquivo `/etc/ssh/sshd_config` com um editor de texto e localize a seguinte linha:

```
#UseDNS yes
```

2. Altere a linha para:

UseDNS no

#### Note

O local desse arquivo de configuração pode diferir para sua distribuição ou se você não estiver executando OpenSSH. Se esse for o caso, consulte a documentação apropriada.

## Identifique-se

Atualmente, não há maneira fácil de saber quem forneceu uma AMI compartilhada, pois cada AMI é representada por um ID de conta.

Recomendamos que você publique uma descrição da sua AMI e o ID da AMI no [Fórum do Amazon EC2](#). Esse é um local central conveniente para usuários que estão interessados em experimentar novas AMIs compartilhadas.

## Proteja-se

Não recomendamos armazenar dados confidenciais ou software em nenhuma AMI compartilhada. Os usuários que executarem uma AMI compartilhada podem ser capazes de reempacotá-la e registrá-la como própria. Siga estas diretrizes para ajudá-lo a evitar alguns riscos de segurança facilmente negligenciados:

- Recomendamos usar a opção `--exclude directory` em `ec2-bundle-vol` para ignorar todos os diretórios e subdiretórios que contêm informações secretas que você não gostaria de incluir no seu pacote. Mais especificamente, exclua todos os arquivos `authorized_keys` de pares de chaves públicas/privadas e SSH de propriedade do usuário ao empacotar a imagem. As AMIs públicas da Amazon armazenam em `/root/.ssh` para a conta raiz e `/home/user_name/.ssh/` para as contas de usuário regulares. Para obter mais informações, consulte [ec2-bundle-vol \(p. 130\)](#).
- Sempre exclua o histórico do shell antes de empacotar. Se você tentar mais de um upload do bundle na mesma AMI, o histórico do shell conterá sua chave de acesso secreta. O exemplo a seguir deve ser o último comando executado antes de empacotar de dentro da instância.

```
[ec2-user ~]$ shred -u ~/.history
```

#### Warning

As limitações de `shred` descritas no alerta acima aplicam-se aqui também.

Esteja ciente de que, ao sair, o bash grava o histórico da sessão atual no disco. Se você fizer `logout` da sua instância após a exclusão de `~/.bash_history`, e depois fizer `login` de volta, descobrirá que `~/.bash_history` foi recriado e contém todos os comandos executados durante a sessão anterior.

Outros programas além do bash também gravam históricos no disco. Use com cuidado e remova ou exclua arquivos-ponto ou diretórios-ponto desnecessários.

- Empacotar uma instância em execução requer sua chave privada e o certificado x.509. Coloque essas e outras credenciais em um local que não seja empacotado (como armazenamento de instâncias).

## AMIs pagas

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 \(p. 103\)](#)
- [Localizar uma AMI paga \(p. 103\)](#)
- [Comprar uma AMI paga \(p. 104\)](#)
- [Obter o código do produto para sua instância \(p. 105\)](#)
- [Usar suporte pago \(p. 105\)](#)
- [Faturas para AMI pagas e compatíveis \(p. 106\)](#)
- [Gerenciar suas assinaturas do AWS Marketplace \(p. 106\)](#)

## 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 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. 533).

## 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 \(p. 533\)](#).

## 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 \(p. 649\)](#).

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

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/product-codes
```

IMDSv1

```
[ec2-user ~]$ curl 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 \(p. 107\)](#)
- [Copiar um AMI \(p. 144\)](#)
- [Armazenar e restaurar uma AMI usando o S3 \(p. 149\)](#)
- [Defasar uma AMI \(p. 155\)](#)
- [Cancelar AMI do Linux \(p. 159\)](#)
- [Automatizar o ciclo de vida da AMI com suporte do EBS \(p. 163\)](#)

## Criar uma AMI

Você pode criar AMIs do Linux baseadas no Amazon EBS e AMIs com armazenamento de instâncias.

### Tópicos

- [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#)
- [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#)

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

## Criar uma AMI do Linux baseada em Amazon EBS

Para criar uma AMI do Linux com Amazon EBS, comece a partir da instância que você executou de uma AMI existente do Linux com Amazon EBS. Pode ser uma AMI que você obteve do AWS Marketplace , uma AMI que você criou usando o [AWS Server Migration Service](#) ou o [VM Import/Export](#), ou qualquer outra AMI à qual você tenha acesso. Depois de personalizar a instância para atender a suas necessidades, crie e registre uma nova AMI, que poderá ser usada para executar novas instâncias com essas personalizações.

Os procedimentos descritos abaixo funcionam para instâncias do Amazon EC2 baseada em volumes do Amazon Elastic Block Store (Amazon EBS) criptografados (incluindo o volume raiz), bem como para volumes descriptografados.

O processo de criação da AMI é diferente para as AMIs com armazenamento de instâncias. Para obter mais informações sobre as diferenças entre instâncias com Amazon EBS e instâncias com armazenamento de instâncias, e como determinar o tipo de dispositivo raiz para sua instância, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#). Para obter mais informações sobre como criar uma AMI do Linux com armazenamento de instâncias, consulte [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#).

Para obter mais informações sobre como criar uma AMI do Windows baseada em Amazon EBS, consulte [Criar uma AMI do Windows baseada em Amazon EBS](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

### Visão geral da criação de AMIs com Amazon EBS

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 corretamente, garanta a integridade dos dados interrompendo a instância antes de criar a AMI e, em seguida, crie a imagem. Quando você cria uma AMI com Amazon EBS, nós a registramos automaticamente para você.

O Amazon EC2 desativa a instância antes de criar a AMI para garantir que tudo na instância seja interrompido e esteja em um estado consistente durante o processo de criação. Se você estiver seguro de que sua instância está em um estado consistente e apropriado para a criação da AMI, poderá informar ao Amazon EC2 para não desativar e reiniciar a instância. Alguns sistemas de arquivos, como o XFS, podem congelar e descongelar atividades, tornando seguro criar a imagem sem reinicializar a instância.

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 AMI do Linux \(p. 159\)](#). Se qualquer volume anexado à instância estiver criptografado, a nova AMI só será executada com êxito em instâncias compatíveis com o Criptografia de Amazon EBS. Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1418\)](#).

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 \(p. 1307\)](#).

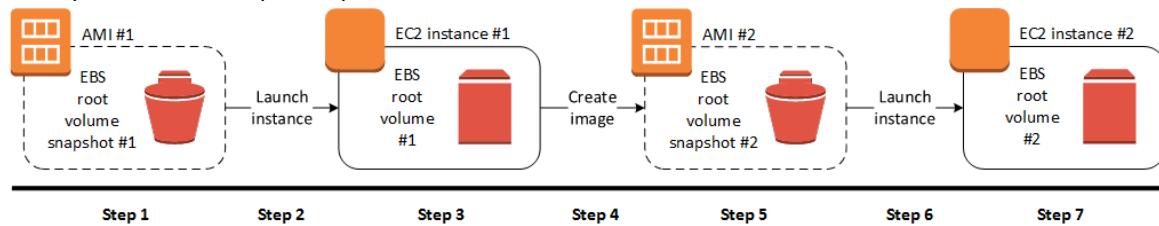
Após a conclusão do processo, uma nova AMI e um snapshot serão criados do volume raiz da instância. Quando você executa uma instância usando a nova AMI, criamos um novo volume do EBS para o volume raiz dele usando o snapshot.

Se você adicionar volumes de armazenamento de instâncias ou volumes do 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 bloco 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 \(p. 1530\)](#).

Ao criar uma nova instância de uma AMI com suporte do EBS, você deve inicializar o volume raiz todo o armazenamento adicional EBS antes de colocá-lo em produção. Para obter mais informações, consulte [Inicializar volumes de Amazon EBS \(p. 1466\)](#).

## Criar uma AMI do Linux a partir de uma instância

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 Amazon EBS a partir de 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.



New console

### Para criar uma AMI de uma instância usando o console

1. Selecione a AMI baseada em EBS apropriada para servir como ponto inicial para a nova AMI e a configure conforme o necessário antes de iniciar. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 510\)](#).
2. Escolha Launch (Executar) para executar a instância da AMI com EBS que você selecionou. 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. \(p. 510\)](#).
3. Quando a instância estiver sendo executada, conecte-se a ela. 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
4. (Opcional) Criar snapshots de todos os volumes anexados à sua instância. Para obter mais informações sobre como criar snapshots, consulte [Criar snapshots de Amazon EBS \(p. 1307\)](#).

5. No painel de navegação, escolha Instances (Instâncias), selecione sua instância e, em seguida, escolha Actions (Ações), Image (Imagem), Create Image (Criar Imagem).

Tip

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

6. Na caixa de diálogo Create Image (Criar imagem), especifique as informações a seguir e escolha Create Image (Criar imagem).

- Image name (Nome da imagem): um nome exclusivo para a imagem.
- Image description (Descrição da imagem): uma descrição opcional da imagem, com até 255 caracteres.
- No reboot (Sem reinicialização): essa opção é selecionada por padrão. O Amazon EC2 encerra a instância, faz snapshots dos volumes anexados, cria e registra a AMI e, em seguida, reinicia a instância. Selecione No reboot (Sem reinicialização) para impedir o encerramento da sua instância.

Warning

Se você selecionar No reboot (Sem reinicialização), a AMI será consistente com falhas (será feito um snapshot de todos os volumes ao mesmo tempo), mas não será consistente com aplicações (nenhum buffer do sistema operacional será liberado para o disco antes que os snapshots sejam criados).

- Instance volumes (Volumes da instância): os campos desta seção permitem que você modifique o volume raiz e adicione outros volumes do Amazon EBS e de armazenamento de instância.
  - O volume raiz é definido na primeira linha. Para alterar o tamanho do volume raiz, em Size (Tamanho), insira o valor necessário.
  - Se você selecionar Delete on Termination (Excluir ao encerrar), quando encerrar a instância criada a partir desta AMI, o volume do EBS será excluído. Se você não selecionar Delete on Termination (Excluir ao encerrar), quando encerrar a instância, o volume do EBS não será excluído. Para obter mais informações, consulte [Preservar volumes do Amazon EBS no encerramento da instância \(p. 591\)](#).
  - Para adicionar o volume do EBS; escolha Add volume (Adicionar volume) (que acrescenta uma nova linha). Em Volume Type (Tipo de volume), escolha EBS e preencha os campos da linha. Quando você executa uma instância da nova AMI, os 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 adicionar um volume de armazenamento de instância, consulte [Adicionar volumes de armazenamento de instâncias a uma AMI \(p. 1505\)](#). Quando você executa uma instância da nova AMI, os 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.
- Tags: você pode marcar a AMI e os snapshots com as mesmas tags ou pode marcá-los com tags diferentes.
  - Para marcar a AMI e os snapshots com as mesmas tags, escolha Tag image and snapshots together (Marcar Imagem e snapshots juntos). As mesmas tags são aplicadas à AMI e a cada snapshot criado.
  - Para marcar a AMI e os snapshots com tags diferentes, escolha Tag image and snapshots separately (Marcar imagem e snapshots separadamente). Diferentes tags são aplicadas à AMI e aos snapshots criados. No entanto, todos os snapshots obtêm as mesmas tags; não é possível marcar cada snapshot com uma tag diferente.

---

(Opcional) Para adicionar uma tag, escolha Add tag (Adicionar tag) e digite a chave e o valor da tag. Repita esse procedimento para cada tag.

7. Para visualizar o status de sua AMI enquanto ela estiver sendo criada, escolha AMIs no painel de navegação. Inicialmente, o status será pending, mas deverá mudar para available após alguns minutos.  
  
(Opcional) Para visualizar o snapshot que foi criado para a nova AMI, escolha Snapshots. Quando você executa uma instância dessa AMI, usamos esse snapshot para criar seu volume do dispositivo raiz.
8. Execute uma instância da nova AMI. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 510\)](#).
9. A nova instância em execução contém todas as personalizações que você aplicou em etapas anteriores.

#### Old console

##### Para criar uma AMI de uma instância usando o console

1. Selecione a AMI baseada em EBS apropriada para servir como ponto inicial para a nova AMI e a configure conforme o necessário antes de iniciar. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 510\)](#).
2. Escolha Launch (Executar) para executar a instância da AMI com EBS que você selecionou. 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. \(p. 510\)](#).
3. Quando a instância estiver sendo executada, conecte-se a ela. 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
4. (Opcional) Criar snapshots de todos os volumes anexados à sua instância. Para obter mais informações sobre como criar snapshots, consulte [Criar snapshots de Amazon EBS \(p. 1307\)](#).
5. No painel de navegação, escolha Instances (Instâncias), selecione sua instância e, em seguida, escolha Actions (Ações), Image (Imagem), Create Image (Criar Imagem).

#### Tip

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

6. Na caixa de diálogo Create Image (Criar imagem), especifique as informações a seguir e escolha Create Image (Criar imagem):
  - Image name (Nome da imagem): um nome exclusivo para a imagem.
  - Image description (Descrição da imagem): uma descrição opcional da imagem, com até 255 caracteres.
  - No reboot (Sem reinicialização): essa opção é selecionada por padrão. O Amazon EC2 encerra a instância, faz snapshots dos volumes anexados, cria e registra a AMI e, em seguida, reinicia a instância. Selecione No reboot (Sem reinicialização) para impedir o encerramento da sua instância.

#### Warning

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

- Instance Volumes (Volumes da instância): os campos nesta seção permitem que você modifique o volume raiz e adicione outros volumes com armazenamento de instância e com Amazon EBS. Para obter informações sobre cada campo, consulte o ícone i próximo a cada campo para mostrar o campo de dicas ferramentas. Alguns aspectos importantes estão listados abaixo.
    - Para alterar o tamanho do volume raiz, localize o volume Root (Raiz) na coluna Volume Type (Tipo de volume) e preencha o campo Size (GiB) (Tamanho (GiB)).
    - Se você selecionar Delete on Termination (Excluir ao encerrar), quando encerrar a instância criada a partir desta AMI, o volume do EBS será excluído. Se você não selecionar Delete on Termination (Excluir ao encerrar), quando encerrar a instância, o volume do EBS não será excluído. Para obter mais informações, consulte [Preservar volumes do Amazon EBS no encerramento da instância \(p. 591\)](#).
    - Para adicionar o volume do EBS; escolha Add New Volume (Adicionar novo volume) (que acrescenta uma nova linha). Em Volume Type (Tipo de volume), escolha EBS e preencha os campos da linha. Quando você executa uma instância da nova AMI, os 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 adicionar um volume de armazenamento de instância, consulte [Adicionar volumes de armazenamento de instâncias a uma AMI \(p. 1505\)](#). Quando você executa uma instância da nova AMI, os 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.
7. Para visualizar o status de sua AMI enquanto ela estiver sendo criada, escolha AMIs no painel de navegação. Inicialmente, o status será pending, mas deverá mudar para available após alguns minutos.
- (Opcional) Para visualizar o snapshot que foi criado para a nova AMI, escolha Snapshots. Quando você executa uma instância dessa AMI, usamos esse snapshot para criar seu volume do dispositivo raiz.
8. Execute uma instância da nova AMI. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 510\)](#).
  9. A nova instância em execução contém todas as personalizações que você aplicou em etapas anteriores.

### 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 AMI do Linux a partir de um snapshot

Se você tiver um snapshot do volume raiz de uma instância, poderá criar uma AMI desse snapshot usando o AWS Management Console ou a linha de comando.

#### Para criar uma AMI de um snapshot usando o console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em Elastic Block Store, escolha Snapshots.
3. Selecione o snapshot e escolha Actions (Ações), Create Image (Criar imagem).

4. Na caixa de diálogo Create Image from EBS Snapshot (Criar imagem de snapshot do EBS), preencha os campos para criar sua AMI e, em seguida, escolha Create (Criar). Se você estiver recriando uma instância-pai, selecione as mesmas opções que a instância-pai.
  - Architecture (Arquitetura): escolha i386 para 32 bits ou x86\_64 para 64 bits.
  - Root device name (Nome do dispositivo raiz): insira o nome apropriado para o volume raiz. Para obter mais informações, consulte [Nomes de dispositivos em instâncias do Linux. \(p. 1528\)](#).
  - Virtualization type (Tipo de virtualização): escolha se as instâncias executadas a partir desta AMI usam virtualização paravirtual (PV) ou máquina virtual de hardware (HVM). Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#).
  - (Somente tipo de virtualização PV) Kernel ID (ID do kernel) e RAM disk ID (ID do disco RAM): escolha AKI e ARI nas listas. Se você escolher a AKI padrão ou não escolher uma AKI, será necessário especificar uma AKI sempre que você executar uma instância usando essa AMI. Além disso, sua instância poderá falhar nas verificações de integridade se a AKI padrão for incompatível com a instância.
  - (Opcional) Block Device Mappings (Mapeamentos de dispositivos de blocos): adicione volumes ou expanda o tamanho padrão do volume raiz para a AMI. Para obter mais informações sobre redimensionamento de arquivo do sistema em sua instância para um volume maior, consulte [Estender um sistema de arquivos Linux após um redimensionamento de volume \(p. 1414\)](#).

Para criar uma AMI 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 \(p. 3\)](#).

- [register-image](#) (AWS CLI)
- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

## Executar uma instância a partir de uma AMI que você criou

Você pode iniciar uma instância a partir de uma AMI criada a partir de uma instância ou snapshot.

Como iniciar uma instância a partir da AMI

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, em Images (Imagens), escolha AMIs.
3. Defina o filtro como Owned by me (De minha propriedade) e selecione sua AMI.
4. Escolha Actions (Ações), Launch (Iniciar).
5. 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. \(p. 510\)](#).

## Criar uma AMI em Linux com armazenamento de instâncias

A AMI que você especifica ao executar a instância determina o tipo de volume do dispositivo raiz

Para criar uma AMI em Linux com armazenamento de instâncias, inicie a instância que você executou a partir de uma AMI em Linux com o armazenamento de instâncias existente. Depois de personalizar a instância para atender às suas necessidades, empacote o volume e registre uma nova AMI, que você pode usar para executar novas instâncias com essas personalizações.

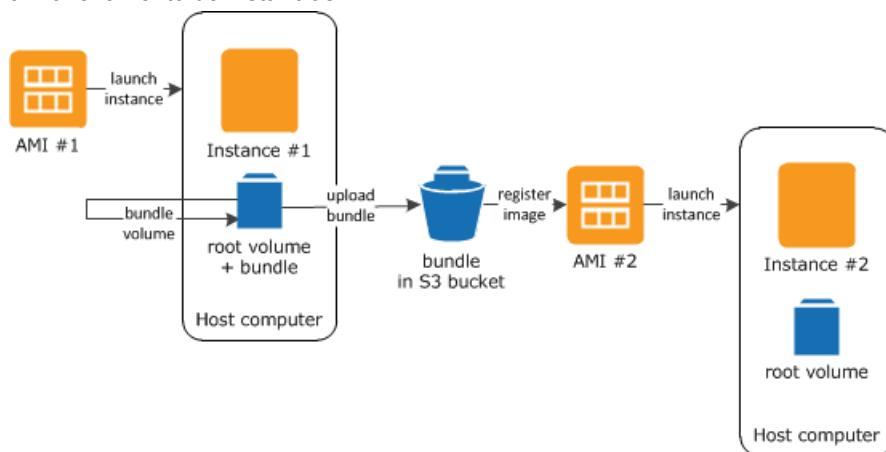
### Important

Somente os seguintes tipos de instância oferecem suporte a um volume de armazenamento de instâncias como o dispositivo raiz: C3, D2, G2, I2, M3 e R3.

O processo de criação da AMI é diferente para AMIs baseadas no Amazon EBS. Para obter mais informações sobre as diferenças entre instâncias com Amazon EBS e instâncias com armazenamento de instâncias, e como determinar o tipo de dispositivo raiz para sua instância, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#). Se você precisar criar uma AMI do Linux com Amazon EBS, consulte [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#).

## Visão geral do processo de criação para AMIs baseadas no armazenamento de instâncias

O diagrama a seguir resume o processo de criação de uma AMI a partir de uma instância com armazenamento de instâncias.



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 forma como você deseja, você pode empacotá-la. Demora vários minutos para o processo de empacotamento ser concluído.

Depois de o processo ser concluído, você terá um pacote, que consiste em um manifesto de imagem (`image.manifest.xml`) e nos arquivos (`image.part.xx`) que contêm um modelo para o volume raiz. Em seguida, você carrega o pacote para seu bucket Amazon S3 e registra sua AMI.

Quando você executa uma instância usando a nova AMI, criamos o volume do dispositivo raiz da instância usando o pacote que você carregou para o Amazon S3. O espaço de armazenamento usado pelo pacote no Amazon S3 gera cobranças na sua conta até que você o exclua. Para obter mais informações, consulte [Cancelar AMI do Linux \(p. 159\)](#).

Se você adicionar volumes de armazenamento de instâncias à sua instância além do volume do dispositivo raiz, o mapeamento de dispositivos de blocos para a nova AMI conterá informações para esses volumes, e os mapeamentos de dispositivos de blocos para as instâncias que você executar pela nova AMI conterão automaticamente informações para esses volumes. Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1530\)](#).

## Prerequisites

Antes que você crie uma AMI, é preciso concluir as tarefas seguir:

- Instale as ferramentas da AMI. Para obter mais informações, consulte [Configurar as ferramentas da AMI \(p. 114\)](#).
- Instale o AWS CLI. Para obter mais informações, consulte [Configuração da AWS Command Line Interface](#).
- Verifique se você tem um bucket Amazon S3 para o pacote. Para criar um bucket do Amazon S3, abra o console do Amazon S3 e clique em Create Bucket (Criar bucket). É possível também usar o comando `mb` da AWS CLI.

- Verifique se você tem seu ID de conta da AWS. Para obter mais informações, consulte [Identificadores de conta da AWS](#) em Referência geral da AWS.
- Certifique-se de que você tem o ID de chave de acesso e a chave de acesso secreta. Para obter mais informações, consulte [Chaves de acesso](#) em Referência geral da AWS.
- Verifique se você tem um certificado x.509 e a chave privada correspondente.
  - Se você precisar criar um certificado X.509, consulte [Gerenciar certificados de assinatura \(p. 116\)](#). O certificado X.509 e a chave privada são usados para criptografar e descriptografar sua AMI.
  - [China (Pequim)] Use o certificado \$EC2\_AMITOOL\_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem.
  - [AWS GovCloud (US-West)] Use o certificado \$EC2\_AMITOOL\_HOME/etc/ec2/amitools/cert-ec2-gov.pem.
- Conecte-se à sua instância e personalize-a. Por exemplo, você pode instalar softwares e aplicações, copiar dados, excluir arquivos temporários e modificar a configuração do Linux.

## Tasks

- [Configurar as ferramentas da AMI \(p. 114\)](#)
- [Criar uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias \(p. 117\)](#)
- [Criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias \(p. 120\)](#)
- [Converter de uma AMI com armazenamento de instâncias em uma AMI com Amazon EBS \(p. 124\)](#)

## Configurar as ferramentas da AMI

Você pode usar os comandos das ferramentas de AMI para criar e gerenciar AMIs do Linux com armazenamento de instâncias. Para usar as ferramentas, você deve instalá-las na sua instância do Linux. As ferramentas das AMIs estão disponíveis como RPM e arquivo .zip para distribuições Linux incompatíveis com RPM.

### Para definir as ferramentas da AMI usando RPM

1. Instale o Ruby usando o gerenciador de pacotes para sua distribuição do Linux, como yum. Por exemplo:

```
[ec2-user ~]$ sudo yum install -y ruby
```

2. Baixe o arquivo RPM usando uma ferramenta como wget ou curl. Por exemplo:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
```

3. Verifique se a assinatura do arquivo RPM está usando o seguinte comando:

```
[ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
```

O comando acima deve indicar que os hashes SHA1 e MD5 do arquivo estão OK. Se o comando indicar que os hashes estão NOT OK, use o seguinte comando para ver os hashes SHA1 e MD5 do cabeçalho do arquivo:

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

Em seguida, compare os hashes SHA1 e MD5 do cabeçalho do arquivo com os seguintes hashes das ferramentas de AMIs verificadas para confirmar a autenticidade do arquivo:

- SHA1 do cabeçalho: a1f662d6f25f69871104e6a62187fa4df508f880

- MD5: 9faff05258064e2f7909b66142de6782

Se os hashes SHA1 e MD5 do cabeçalho do arquivo corresponder aos hashes das ferramentas de AMI verificadas, vá para a próxima etapa.

4. Instale o RPM usando o comando a seguir:

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. Verifique a instalação das suas ferramentas da AMI usando o comando [ec2-ami-tools-version \(p. 127\)](#).

```
[ec2-user ~]$ ec2-ami-tools-version
```

#### Note

Se você receber um erro de carregamento, como "não é possível carregar esse arquivo -- ec2/amitools/version (LoadError)", realize a próxima etapa para adicionar o local de instalação das suas ferramentas da AMI para seu RUBYLIB caminho.

6. (Opcional) Se você tiver recebido um erro na etapa anterior, adicione a localização das suas ferramentas da AMI para seu caminho RUBYLIB.
  - a. Execute o comando a seguir para determinar os caminhos a adicionar.

```
[ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
/usr/lib/ruby/site_ruby/ec2/amitools/version.rb
/usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
```

No exemplo acima, o arquivo ausente no erro de carga anterior está localizado em /usr/lib/ruby/site\_ruby e /usr/lib64/ruby/site\_ruby.

- b. Adicione os locais da etapa anterior ao seu caminho de RUBYLIB.

```
[ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/
site_ruby
```

- c. Verifique a instalação das suas ferramentas da AMI usando o comando [ec2-ami-tools-version \(p. 127\)](#).

```
[ec2-user ~]$ ec2-ami-tools-version
```

Para configurar as ferramentas da AMI usando o arquivo .zip

1. Instale o Ruby e descompacte usando o gerenciador de pacotes para sua distribuição do Linux, como apt-get. Por exemplo:

```
[ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. Baixe o arquivo .zip usando uma ferramenta como wget ou curl. Por exemplo:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. Descompacte os arquivos em um diretório de instalação apropriado, como /usr/local/ec2.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
```

```
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

Observe que o arquivo .zip contém uma pasta ec2-ami-tools-**x.x.x**, em que **x.x.x** é o número da versão das ferramentas (por exemplo, ec2-ami-tools-1.5.7).

4. Ajuste a variável de ambiente EC2\_AMITOOL\_HOME para o diretório de instalação para as ferramentas. Por exemplo:

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Adicione as ferramentas à sua variável de ambiente PATH. Por exemplo:

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. Você pode verificar a instalação das suas ferramentas da AMI usando o comando [ec2-ami-tools-version \(p. 127\)](#).

```
[ec2-user ~]$ ec2-ami-tools-version
```

## Gerenciar certificados de assinatura

Determinados comandos nas ferramentas da AMI exigem a assinatura de um certificado (também conhecido como certificado X.509). Você deve criar o certificado e, então, carregá-lo para a AWS. Por exemplo, você pode usar uma ferramenta de terceiros, como OpenSSL, para criar o certificado.

### Para criar um certificado de assinatura

1. Instale e configure o OpenSSL.
2. Crie uma chave privada usando o comando openssl genrsa e salve a saída em um arquivo .pem. Recomendamos que você crie uma chave RSA de 2048 ou 4096 bits.

```
openssl genrsa 2048 > private-key.pem
```

3. Gere um certificado usando o comando openssl req.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -out certificate.pem
```

Para carregar o certificado para a AWS, use o comando [upload-signing-certificate](#).

```
aws iam upload-signing-certificate --user-name user-name --certificate-body file://path/to/certificate.pem
```

Para listar os certificados para um usuário, use o comando [list-signing-certificates](#):

```
aws iam list-signing-certificates --user-name user-name
```

Para desabilitar ou reabilitar um certificado de assinatura para um usuário, use o comando [update-signing-certificate](#). O comando a seguir desabilita o certificado:

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE --status Inactive --user-name user-name
```

Para excluir um certificado, use o comando [delete-signing-certificate](#):

```
aws iam delete-signing-certificate --user-name user-name --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE
```

## Criar uma AMI a partir de uma instância com armazenamento de instâncias

Os procedimentos a seguir são para criar uma AMI com armazenamento de instâncias com base na instância com armazenamento de instâncias. Antes de começar, certifique-se de que você leu os [Pré-requisitos \(p. 113\)](#).

### Tópicos

- [Criar uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias \(p. 117\)](#)
- [Criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias \(p. 120\)](#)

## Criar uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias

Esta seção descreve a criação da AMI a partir de uma instância do Amazon Linux. Os procedimentos a seguir podem não funcionar para instâncias que executam outras distribuições do Linux. Para procedimentos específicos do Ubuntu, consulte [Criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias \(p. 120\)](#).

Para se preparar para usar as ferramentas da AMI (somente instâncias do HVM)

1. As ferramentas de AMI exigem GRUB Legacy para inicializarem corretamente. Use o comando a seguir para instalar o GRUB:

```
[ec2-user ~]$ sudo yum install -y grub
```

2. Instale os pacotes de gerenciamento de partição com o seguinte comando:

```
[ec2-user ~]$ sudo yum install -y gdisk kpartx parted
```

Para criar uma AMI a partir de uma instância de Amazon Linux com armazenamento de instâncias

Este procedimento pressupõe que você atendeu aos pré-requisitos de [Prerequisites \(p. 113\)](#).

1. Carregue suas credenciais para sua instância. Usamos essas credenciais para garantir que só você e o Amazon EC2 possam acessar sua AMI.
  - a. Crie um diretório temporário na sua instância para suas credenciais, da seguinte forma:

```
[ec2-user ~]$ mkdir /tmp/cert
```

Isso permite que você exclua suas credenciais da imagem criada.

- b. Copie o certificado X.509 e a chave privada correspondente do seu computador para o diretório /tmp/cert na sua instância usando uma ferramenta de cópia segura, como [scp \(p. 539\)](#). A opção `-i my-private-key.pem` no comando `scp` é a chave privada que você usa para se conectar à sua instância com o SSH, não a chave privada X.509. Por exemplo:

```
you@your_computer:~ $ scp -i my-private-key.pem /  
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /  
path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-  
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/  
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 717 0.7KB/s 00:00
```

```
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 685 0.7KB/s 00:00
```

Como alternativa, por serem arquivos de texto simples, você pode abrir o certificado e a chave em um editor de texto e copiar o conteúdo para novos arquivos em /tmp/cert.

2. Prepare o pacote para carregar para o Amazon S3 executando o comando [ec2-bundle-vol \(p. 130\)](#) de dentro da sua instância. Não se esqueça de especificar a opção `-e` para de excluir o diretório onde suas credenciais estão armazenadas. Por padrão, o processo de colocação em pacotes exclui arquivos que possam conter informações confidenciais. Esses arquivos incluem `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*`, `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` e `*/.bash_history`. Para incluir todos os arquivos, use a opção `--no-filter`. Para incluir alguns dos arquivos, use a opção `--include`.

#### Important

Por padrão, o processo de empacotamento da AMI cria um conjunto de arquivos compactados e criptografados no diretório /tmp que representa o volume raiz. Se você não tem o espaço em disco suficiente em /tmp para armazenar o pacote, precisa especificar um local diferente para o pacote ser armazenado com a opção `-d /path/to/bundle/storage`. Algumas instâncias têm armazenamento temporário montado em /mnt ou /media/ephemeral0 que você pode usar, ou você pode também [criar \(p. 1274\)](#), [associar \(p. 1277\)](#) e [montar \(p. 1283\)](#) um novo volume do Amazon Elastic Block Store (Amazon EBS) para armazenar o pacote.

- a. Você deve executar o comando ec2-bundle-vol como raiz. Na maioria dos comandos, você pode usar sudo para ganhar permissões elevadas, mas neste caso, você deve executar sudo -E su para manter as variáveis do ambiente.

```
[ec2-user ~]$ sudo -E su
```

Observe que prompt bash agora identifica você como usuário raiz, e o cifrão foi substituído por uma hashtag, sinalizando que você está em um shell raiz:

```
[root ec2-user]#
```

- b. Para criar o pacote de AMIs, execute o comando [ec2-bundle-vol \(p. 130\)](#) da seguinte forma:

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --partition gpt
```

#### Note

Para as regiões China (Pequim) e AWS GovCloud (US-West), use o parâmetro `--ec2cert` e especifique os certificados de acordo com os [pré-requisitos \(p. 113\)](#).

Pode demorar alguns minutos para criar a imagem. Quando esse comando for concluído, o diretório /tmp (ou não padrão) conterá o pacote (`image.manifest.xml`, além de vários arquivos `image.part.xx`).

- c. Saída do shell raiz.

```
[root ec2-user]# exit
```

3. (Opcional) Para adicionar mais volumes de armazenamento de instâncias, edite os mapeamentos de dispositivos de blocos no arquivo `image.manifest.xml` para sua AMI. Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1530\)](#).

- a. Crie um backup do seu arquivo `image.manifest.xml`.

```
[ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

- b. Reformate o arquivo `image.manifest.xml` para que seja mais fácil ler e editar.

```
[ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/image.manifest.xml
```

- c. Edite os mapeamentos de dispositivos de blocos em `image.manifest.xml` com um editor de texto. O exemplo abaixo mostra uma nova entrada para o volume do armazenamento de instâncias `ephemeral1`.

Note

Para obter uma lista dos arquivos excluídos, consulte [ec2-bundle-vol \(p. 130\)](#).

```
<block_device_mapping>
  <mapping>
    <virtual>ami</virtual>
    <device>sda</device>
  </mapping>
  <mapping>
    <virtual>ephemeral0</virtual>
    <device>sdb</device>
  </mapping>
  <mapping>
    <virtual>ephemeral1</virtual>
    <device>sdc</device>
  </mapping>
  <mapping>
    <virtual>root</virtual>
    <device>/dev/sda1</device>
  </mapping>
</block_device_mapping>
```

- d. Salve o arquivo `image.manifest.xml` e saia do seu editor de texto.
4. Para fazer upload do pacote para o Amazon S3, execute o comando [ec2-upload-bundle \(p. 140\)](#) da seguinte forma.

```
[ec2-user ~]$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

Important

Para registrar a AMI em uma região diferente de US East (N. Virginia), é preciso especificar tanto a região de destino com a opção `--region` quanto um caminho do bucket que já exista na região de destino, ou um caminho de bucket exclusivo que possa ser criado na região de destino.

5. (Opcional) Depois de o pacote ser carregado para o Amazon S3, você pode removê-lo do diretório `/tmp` na instância usando o comando `rm` a seguir:

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

**Important**

Se você tiver especificado um caminho com a opção `-d /path/to/bundle/storage` em [Step 2 \(p. 118\)](#), use esse caminho em vez de `/tmp`.

6. Para registrar a AMI, execute o comando `register-image` da seguinte maneira.

```
[ec2-user ~]$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --virtualization-
type hvm
```

**Important**

Se você tiver especificado previamente uma região para o comando `ec2-upload-
bundle` ([p. 140](#)), especifique essa região novamente para esse comando.

### Criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias

Esta seção descreve a criação de uma AMI a partir de uma instância Ubuntu Linux com um volume de armazenamento de instâncias como o volume raiz. Os procedimentos a seguir podem não funcionar para instâncias que executam outras distribuições do Linux. Para obter procedimentos específicos para o Amazon Linux, consulte [Criar uma AMI a partir de uma instância do Amazon Linux com armazenamento de instâncias \(p. 117\)](#).

Para se preparar para usar as ferramentas da AMI (somente instâncias do HVM)

As ferramentas de AMI exigem GRUB Legacy para inicializarem corretamente. Contudo, o Ubuntu está configurado para usar GRUB 2. Você deve verificar se sua instância usa GRUB Legacy e, caso negativo, é preciso instalá-lo e configurá-lo.

As instâncias de HVM também exigem a instalação de ferramentas de particionamento para as ferramentas de AMI funcionarem corretamente.

1. O GRUB Legacy (versão 0.9x ou anterior) deve estar instalado na sua instância. Verifique se o GRUB Legacy está presente e instale-o, se necessário.

- a. Verifique a versão da sua instalação do GRUB.

```
ubuntu:~$ grub-install --version
grub-install (GRUB) 1.99-21ubuntu3.10
```

Neste exemplo, a versão do GRUB é posterior à 0.9x, de modo que você deve instalar o GRUB Legacy. Vá para [Step 1.b \(p. 120\)](#). Se o GRUB Legacy já estiver presente, vá direto para [Step 2 \(p. 120\)](#).

- b. Instale o pacote grub usando o comando a seguir.

```
ubuntu:~$ sudo apt-get install -y grub
```

2. Instale os pacotes de gerenciamento de partição a seguir usando o gerenciador de pacotes para sua distribuição.

- gdisk (algumas distribuições podem acessar o pacote gptfdisk em seu lugar)
- kpartx
- parted

Use o seguinte comando.

```
ubuntu:~$ sudo apt-get install -y gdisk kpartx parted
```

3. Verifique os parâmetros do kernel para sua instância.

```
ubuntu:~$ cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-3.2.0-54-virtual root=UUID=4f392932-ed93-4f8f-
aee7-72bc5bb6ca9d ro console=ttyS0 xen_emul_unplug=unnecessary
```

Observe as opções após o kernel e os parâmetros do dispositivo raiz: `ro`, `console=ttyS0` e `xen_emul_unplug=unnecessary`. Suas opções podem diferir.

4. Verifique as entradas do kernel em `/boot/grub/menu.lst`.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=hvc0
kernel /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
kernel /boot/memtest86+.bin
```

Observe se o parâmetro `console` está apontando para `hvc0` em vez de `ttyS0` e se o parâmetro `xen_emul_unplug=unnecessary` está ausente. Mais uma vez, suas opções podem diferir.

5. Edite o arquivo `/boot/grub/menu.lst` com seu editor de texto favorito (como o vim ou o nano) para alterar o `console` e adicionar os parâmetros identificados anteriormente às entradas de inicialização.

```
title      Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual
root      (hd0)
kernel    /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs
          ro console=ttyS0 xen_emul_unplug=unnecessary
initrd   /boot/initrd.img-3.2.0-54-virtual

title      Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual (recovery mode)
root      (hd0)
kernel    /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro
          single console=ttyS0 xen_emul_unplug=unnecessary
initrd   /boot/initrd.img-3.2.0-54-virtual

title      Ubuntu 12.04.3 LTS, memtest86+
root      (hd0)
kernel    /boot/memtest86+.bin
```

6. Verifique se suas entradas de kernel agora contêm os parâmetros corretos.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=ttyS0
          xen_emul_unplug=unnecessary
kernel /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
          console=ttyS0 xen_emul_unplug=unnecessary
kernel /boot/memtest86+.bin
```

7. [Somente para Ubuntu 14.04 e mais recentes] Começando pelo Ubuntu 14.04, AMIs do Ubuntu suportadas pelo armazenamento de instâncias usam uma tabela de partição de GPT e uma partição de EFI separado montados em `/boot/efi`. O comando `ec2-bundle-vol` não empacotará essa partição de inicialização, portanto você precisa comentar a entrada `/etc/fstab` para a partição EFI, conforme exibido no exemplo a seguir.

```
LABEL=cloudimg-rootfs   /           ext4   defaults          0 0
#LABEL=UEFI            /boot/efi     vfat    defaults          0 0
/dev/xvdb             /mnt        auto    defaults,nobootwait,comment=cloudconfig 0          2
```

Para criar uma AMI a partir de uma instância em Ubuntu com armazenamento de instâncias

Este procedimento pressupõe que você atendeu aos pré-requisitos de [Prerequisites \(p. 113\)](#).

1. Carregue suas credenciais para sua instância. Usamos essas credenciais para garantir que só você e o Amazon EC2 possam acessar sua AMI.
  - a. Crie um diretório temporário na sua instância para suas credenciais, da seguinte forma:

```
ubuntu:~$ mkdir /tmp/cert
```

Isso permite que você exclua suas credenciais da imagem criada.

- b. Copie a chave privada e o certificado X.509 do seu computador para o diretório `/tmp/cert` na sua instância usando uma ferramenta de cópia segura, como a [scp \(p. 539\)](#). A opção `-i my-private-key.pem` no comando `scp` é a chave privada que você usa para se conectar à sua instância com o SSH, não a chave privada X.509. Por exemplo:

```
you@your_computer:~ $ scp -i my-private-key.pem /  
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /  
path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-  
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/  
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 717 0.7KB/s 00:00  
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 685 0.7KB/s 00:00
```

Como alternativa, por serem arquivos de texto simples, você pode abrir o certificado e a chave em um editor de texto e copiar o conteúdo para novos arquivos em `/tmp/cert`.

2. Prepare o pacote para fazer upload para o Amazon S3 executando o comando [ec2-bundle-vol \(p. 130\)](#) a partir de sua instância. Não se esqueça de especificar a opção `-e` para de excluir o diretório onde suas credenciais estão armazenadas. Por padrão, o processo de colocação em pacotes exclui arquivos que possam conter informações confidenciais. Esses arquivos incluem `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*.id_rsa*`, `*.id_dsa*`, `*.gpg`, `*.jks`, `*.ssh/authorized_keys` e `*/.bash_history`. Para incluir todos os arquivos, use a opção `--no-filter`. Para incluir alguns dos arquivos, use a opção `--include`.

#### Important

Por padrão, o processo de empacotamento da AMI cria um conjunto de arquivos compactados e criptografados no diretório `/tmp` que representa o volume raiz. Se você não tem o espaço em disco suficiente em `/tmp` para armazenar o pacote, precisa especificar um local diferente para o pacote ser armazenado com a opção `-d /path/to/bundle/storage`. Algumas instâncias têm armazenamento temporário montado em `/mnt` ou `/media/ephemeral0` que você pode usar, ou você pode também [criar \(p. 1274\)](#), [associar \(p. 1277\)](#) e [montar \(p. 1283\)](#) um novo volume do Amazon Elastic Block Store (Amazon EBS) para armazenar o pacote.

- a. Você deve executar o comando `ec2-bundle-vol` como raiz. Na maioria dos comandos, você pode usar `sudo` para ganhar permissões elevadas, mas neste caso, você deve executar `sudo -E` su para manter as variáveis do ambiente.

```
ubuntu:~$ sudo -E su
```

Observe que prompt bash agora identifica você como usuário raiz, e o cifrão foi substituído por uma hashtag, sinalizando que você está em um shell raiz:

```
root@ubuntu:#
```

- b. Para criar o pacote de AMIs, execute o comando [ec2-bundle-vol \(p. 130\)](#) da seguinte forma.

```
root@ubuntu:# ec2-bundle-vol -k /tmp/cert/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  
-c /tmp/cert/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u your_aws_account_id -r  
x86_64 -e /tmp/cert --partition gpt
```

**Important**

Para Ubuntu 14.04 e as instâncias HVM posteriores, adicione o marcador `--partition mbr` para empacotar as instruções de inicialização corretamente; caso contrário, sua AMI recém-criada não inicializará.

Pode demorar alguns minutos para criar a imagem. Quando esse comando for concluído, o diretório `tmp` conterá o pacote (`image.manifest.xml`, além de vários arquivos `image.part.xx`).

- c. Saída do shell raiz.

```
root@ubuntu:# exit
```

3. (Opcional) Para adicionar mais volumes de armazenamento de instâncias, edite os mapeamentos de dispositivos de blocos no arquivo `image.manifest.xml` para sua AMI. Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1530\)](#).

- a. Crie um backup do seu arquivo `image.manifest.xml`.

```
ubuntu:~$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
```

- b. Reformate o arquivo `image.manifest.xml` para que seja mais fácil ler e editar.

```
ubuntu:~$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/  
image.manifest.xml
```

- c. Edite os mapeamentos de dispositivos de blocos em `image.manifest.xml` com um editor de texto. O exemplo abaixo mostra uma nova entrada para o volume do armazenamento de instâncias `ephemeral1`.

```
<block_device_mapping>  
  <mapping>  
    <virtual>ami</virtual>  
    <device>sda</device>  
  </mapping>  
  <mapping>  
    <virtual>ephemeral0</virtual>  
    <device>sdb</device>  
  </mapping>  
  <mapping>  
    <virtual>ephemeral1</virtual>  
    <device>sdc</device>  
  </mapping>  
  <mapping>  
    <virtual>root</virtual>  
    <device>/dev/sda1</device>  
  </mapping>  
</block_device_mapping>
```

- d. Salve o arquivo `image.manifest.xml` e saia do seu editor de texto.

4. Para fazer upload do pacote para o Amazon S3, execute o comando [ec2-upload-bundle \(p. 140\)](#) da seguinte forma.

```
ubuntu:~$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/  
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

**Important**

Se você pretende registrar a AMI em uma região diferente de US East (N. Virginia), é preciso especificar tanto a região de destino com a opção `--region` quanto um caminho do bucket que já exista na região de destino, ou um caminho de bucket exclusivo que possa ser criado na região de destino.

5. (Opcional) Depois de o pacote ser carregado para o Amazon S3, você pode removê-lo do diretório `/tmp` na instância usando o comando `rm` a seguir:

```
ubuntu:~$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

**Important**

Se você tiver especificado um caminho com a opção `-d` `/path/to/bundle/storage` em [Step 2 \(p. 122\)](#), use o mesmo caminho abaixo, em vez de `/tmp`.

6. Para registrar a AMI, execute o comando `register-image` da AWS CLI da seguinte maneira.

```
ubuntu:~$ aws ec2 register-image --image-location my-s3-  
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --virtualization-  
type hvm
```

**Important**

Se você tiver especificado previamente uma região para o comando [ec2-upload-bundle \(p. 140\)](#), especifique essa região novamente para esse comando.

7. [Ubuntu 14.04 e posterior] Retire a entrada EFI em `/etc/fstab`; caso contrário, sua instância em execução não conseguirá reiniciar.

## Converter de uma AMI com armazenamento de instâncias em uma AMI com Amazon EBS

Você pode converter uma AMI do Linux com armazenamento de instâncias em uma AMI do Linux com Amazon EBS.

**Important**

Você não pode converter uma AMI do Windows com armazenamento de instâncias em uma AMI do Windows com Amazon EBS, nem converter uma AMI que não seja sua.

Para converter uma AMI com armazenamento de instâncias em uma AMI com Amazon EBS

1. Execute uma instância do Amazon Linux a partir de uma AMI com Amazon EBS. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 510\)](#). As instâncias do Amazon Linux têm a AWS CLI e as ferramentas da AMI pré-instaladas.
2. Carregue a chave privada X.509 usada para empacotar sua AMI com armazenamento de instâncias para sua instância. Usamos essa chave para garantir que só você e o Amazon EC2 possam acessar sua AMI.
  - a. Crie um diretório temporário na sua instância para a chave privada X.509 da seguinte forma:

```
[ec2-user ~]$ mkdir /tmp/cert
```

- b. Copie a chave privada X.509 do seu computador para o diretório /tmp/cert na sua instância usando uma ferramenta de cópia segura, como a [scp \(p. 539\)](#). O parâmetro *my-private-key* no comando a seguir é a chave privada que você usa para se conectar à sua instância com o SSH. Por exemplo:

```
you@your_computer:~ $ scp -i my-private-key.pem /  
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-  
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/  
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem 100% 717 0.7KB/s 00:00
```

3. Defina as variáveis de ambiente para sua chave de acesso da AWS e uma chave secreta.

```
[ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id  
[ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
```

4. Prepare um volume do Amazon Elastic Block Store (Amazon EBS) para sua nova AMI.

- a. Crie um o volume do EBS vazio na mesma zona de disponibilidade que sua instância usando o comando [create-volume](#). Observe o ID do volume na saída do comando.

**Important**

Esse volume do EBS deve ter tamanho igual ou superior ao volume do dispositivo raiz do armazenamento de instâncias original.

```
[ec2-user ~]$ aws ec2 create-volume --size 10 --region us-west-2 --availability-zone us-west-2b
```

- b. Associe o volume à sua instância com Amazon EBS usando o comando [attach-volume](#).

```
[ec2-user ~]$ aws ec2 attach-volume --volume-id volume_id --instance-id instance_id  
--device /dev/sdb --region us-west-2
```

5. Crie uma pasta para o seu pacote.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Baixe o pacote para sua AMI com armazenamento de instâncias para /tmp/bundle usando o comando [ec2-download-bundle](#) (p. 136).

```
[ec2-user ~]$ ec2-download-bundle -b my-s3-bucket/bundle_folder/bundle_name -m  
image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --privatekey /path/  
to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Reconstitua o arquivo de imagem do pacote usando o comando [ec2-unbundle](#) (p. 140).

- a. Altere os diretórios para a pasta de pacotes.

```
[ec2-user ~]$ cd /tmp/bundle/
```

- b. Execute o comando [ec2-unbundle](#) (p. 140).

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-  
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. Copie os arquivos da imagem não empacotada para o novo volume do EBS.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Teste o volume quanto a quaisquer novas partições não empacotadas.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Liste os dispositivos de blocos para encontrar o nome do dispositivo para montar.

```
[ec2-user bundle]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0   0   8G  0 disk
##/dev/sda1 202:1   0   8G  0 part /
/dev/sdb    202:80  0  10G  0 disk
##/dev/sdb1 202:81  0  10G  0 part
```

Neste exemplo, a partição a montar é /dev/sdb1, mas o nome do seu dispositivo provavelmente será diferente. Se seu volume não estiver particionado, o dispositivo para montar será semelhante a /dev/sdb (sem um dígito final de partição do dispositivo).

11. Crie um ponto de montagem para o novo volume do EBS e monte o volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Abra o arquivo /etc/fstab no volume do EBS com seu editor de texto favorito (como o vim ou o nano) e remova todas as entradas dos volumes de armazenamento de instâncias (temporários). Como o volume do EBS é montado em /mnt/ebs, o arquivo fstab é localizado em /mnt/ebs/etc/fstab.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/      /          ext4    defaults,noatime 1  1
tmpfs        /dev/shm   tmpfs   defaults        0  0
devpts       /dev/pts   devpts  gid=5,mode=620 0  0
sysfs        /sys       sysfs   defaults        0  0
proc         /proc      proc    defaults        0  0
/dev/sdb     /media/ephemeral0 auto    defaults,comment=cloudconfig 0
2
```

Neste exemplo, a última linha deve ser removida.

13. Desmonte o volume e separe-o da instância.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id volume_id --region us-west-2
```

14. Crie uma AMI a partir do novo volume do EBS, da seguinte forma.

- Crie um snapshot do novo volume do EBS.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
"your_snapshot_description" --volume-id volume_id
```

- Verifique se seu snapshot está concluído.

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
id snapshot_id
```

- c. Identifique a arquitetura do processador, o tipo de virtualização e a imagem do kernel (aki) usados na AMI original com o comando `describe-images`. Para esta etapa, você precisa do ID da AMI com armazenamento de instâncias original.

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-id ami-id --output text
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon available
public machine aki-fc8f11cc instance-store paravirtual xen
```

Neste exemplo, arquitetura é `x86_64` e o ID da imagem do kernel é `aki-fc8f11cc`. Use os valores a seguir na próxima etapa. Se a saída do comando acima também listar um ID `ari`, anote isso também.

- d. Registre sua nova AMI com o ID do snapshot do seu novo volume do EBS e os valores da etapa anterior. Se a saída do comando anterior listou um ID `ari`, inclua-o no comando seguinte com `--ramdisk-id ari_id`.

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --name your_new_ami_name --block-device-mappings DeviceName=device-name,Ebs={SnapshotId=snapshot_id} --virtualization-type paravirtual --architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Opcional) Depois de ter testado que pode executar uma instância a partir da nova AMI, você pode excluir o volume do EBS criado para esse procedimento.

```
aws ec2 delete-volume --volume-id volume_id
```

## Referência de ferramentas da AMI

Você pode usar os comandos das ferramentas da AMI para criar e gerenciar AMIs em Linux com armazenamento de instâncias. Para configurar as ferramentas, consulte [Configurar as ferramentas da AMI \(p. 114\)](#).

Para obter informações sobre suas chaves de acesso, consulte [Práticas recomendadas para gerenciar as chaves de acesso da AWS](#).

### Comandos

- [ec2-ami-tools-version \(p. 127\)](#)
- [ec2-bundle-image \(p. 128\)](#)
- [ec2-bundle-vol \(p. 130\)](#)
- [ec2-delete-bundle \(p. 134\)](#)
- [ec2-download-bundle \(p. 136\)](#)
- [ec2-migrate-manifest \(p. 138\)](#)
- [ec2-unbundle \(p. 140\)](#)
- [ec2-upload-bundle \(p. 140\)](#)
- [Opções comuns de ferramentas da AMI \(p. 143\)](#)

### ec2-ami-tools-version

#### Description

Descreve a versão das ferramentas da AMI.

## Syntax

```
ec2-ami-tools-version
```

## Output

As informações da versão.

## Example

Este comando de exemplo exibe as informações da versão das ferramentas de AMI que você está usando.

```
[ec2-user ~]$ ec2-ami-tools-version
1.5.2 20071010
```

## ec2-bundle-image

### Description

Crie uma AMI em Linux com armazenamento de instâncias a partir de uma imagem de sistema operacional criada em um arquivo de loopback.

### Syntax

```
ec2-bundle-image -c path -k path -u account -i path [-d path] [--ec2cert path]
[-r architecture] [--productcodes code1,code2,...] [-B mapping] [-p prefix]
```

### Options

**-c, --cert path**

O arquivo de certificado de chave pública RSA codificado por PEM do usuário.

Obrigatório: sim

**-k, --privatekey path**

O caminho para um arquivo de chave RSA codificado por PEM. Será necessário especificar essa chave para desfazer esse pacote e, assim, mantê-lo em um lugar seguro. Observe que a chave não precisa estar registrada na conta da AWS.

Obrigatório: sim

**-u, --user account**

O ID da conta da AWS do usuário, sem traços.

Obrigatório: sim

**-i, --image path**

O caminho até imagem para fazer o pacote.

Obrigatório: sim

**-d, --destination path**

O diretório no qual o pacote deve ser criado.

Padrão: /tmp

Exigido: Não

**--ec2cert path**

O caminho até o certificado de chave pública X.509 do Amazon EC2 usado para criptografar o manifesto da imagem.

As regiões `us-gov-west-1` e `cn-north-1` usam um certificado de chave pública não padrão e o caminho para esse certificado deve ser especificado com essa opção. O caminho para o certificado varia de acordo com o método de instalação das ferramentas da AMI. Para o Amazon Linux, os certificados estão localizados em `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se você tiver instalado as ferramentas da AMI do arquivo RPM ou ZIP em [Configurar as ferramentas da AMI \(p. 114\)](#), os certificados estarão localizados em `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obrigatório: apenas para as regiões `us-gov-west-1` e `cn-north-1`.

**-r, --arch architecture**

Arquitetura da imagem. Se você não tiver fornecido a arquitetura na linha de comando, ela será solicitada quando o empacotamento for iniciado.

Valores válidos: `i386` | `x86_64`

Exigido: Não

**--productcodes code1,code2,...**

Os códigos de produto para associar à imagem no momento do registro, separado por vírgulas.

Exigido: Não

**-B, --block-device-mapping mapping**

Define como dispositivos de blocos são expostos a uma instância dessa AMI, caso esse tipo de instância seja compatível com o dispositivo especificado.

Especifique uma lista separada por vírgulas de pares de valor-chave, nos quais cada chave é um nome virtual e cada valor é o nome do dispositivo correspondente. Os nomes virtuais incluem o seguinte:

- `ami` — o dispositivo do sistema de arquivos raiz, como visto pela instância
- `root` — o dispositivo do sistema de arquivos raiz, como visto pelo kernel
- `swap` — o dispositivo de troca, como visto pela instância
- `ephemeralN` — o enésimo volume de armazenamento de instâncias

Exigido: Não

**-p, --prefix prefix**

O prefixo do nome dos arquivos de AMI em pacote.

Padrão: O nome de arquivo de imagem. Por exemplo: se o caminho da imagem for `/var/spool/my-image/version-2/debian.img`, o prefixo padrão será `debian`.`img`.

Exigido: Não

**--kernel kernel\_id**

Suspenso. Use [register-image](#) para configurar o kernel.

Exigido: Não

**--ramdisk ramdisk\_id**

Suspenso. Use [register-image](#) para configurar o disco RAM, se necessário.

Exigido: Não

## Output

Mensagens de status que descrevem os estágios e o status do processo de empacotamento.

### Example

Este exemplo cria uma AMI empacotada a partir de uma imagem de sistema operacional criada em um arquivo de loopback.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

## ec2-bundle-vol

### Description

Cria uma AMI em Linux com armazenamento de instâncias ao compactar, criptografar e assinar uma cópia do volume do dispositivo raiz da instância.

O Amazon EC2 tenta herdar códigos de produto, configurações de kernel, configurações do disco RAM e mapeamentos de dispositivos de blocos a partir da instância.

Por padrão, o processo de colocação em pacotes exclui arquivos que possam conter informações confidenciais. Esses arquivos incluem \*.sw, \*.swo, \*.swp, \*.pem, \*.priv, \*id\_rsa\*, \*id\_dsa\*, \*.gpg, \*.jks, \*/.ssh/authorized\_keys e \*/.bash\_history. Para incluir todos os arquivos, use a opção --no-filter. Para incluir alguns dos arquivos, use a opção --include.

Para obter mais informações, consulte [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#).

### Syntax

```
ec2-bundle-vol -c path -k path -u account [-d path] [--ec2cert path] [-r architecture] [--productcodes code1,code2,...] [-B mapping] [--all] [-e directory1,directory2,...] [-i file1,file2,...] [--no-filter] [-p prefix] [-s size] [--[no-]inherit] [-v volume] [-P type] [-S script] [--fstab path] [--generate-fstab] [--grub-config path]
```

## Options

**-c, --cert path**

O arquivo de certificado de chave pública RSA codificado por PEM do usuário.

Obrigatório: sim

**-k, --privatekey path**

O caminho até o arquivo de chaves RSA codificado por PEM do usuário.

Obrigatório: sim

**-u, --user account**

O ID da conta da AWS do usuário, sem traços.

Obrigatório: sim

**-d, --destination destination**

O diretório no qual o pacote deve ser criado.

Padrão: /tmp

Exigido: Não

**--ec2cert path**

O caminho até o certificado de chave pública X.509 do Amazon EC2 usado para criptografar o manifesto da imagem.

As regiões `us-gov-west-1` e `cn-north-1` usam um certificado de chave pública não padrão e o caminho para esse certificado deve ser especificado com essa opção. O caminho para o certificado varia de acordo com o método de instalação das ferramentas da AMI. Para o Amazon Linux, os certificados estão localizados em `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se você tiver instalado as ferramentas da AMI do arquivo RPM ou ZIP em [Configurar as ferramentas da AMI \(p. 114\)](#), os certificados estarão localizados em `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obrigatório: apenas para as regiões `us-gov-west-1` e `cn-north-1`.

**-r, --arch architecture**

A arquitetura da imagem. Se você não tiver fornecido isso na linha de comando, ela será solicitada a fornecer quando o empacotamento for iniciado.

Valores válidos: `i386` | `x86_64`

Exigido: Não

**--productcodes code1,code2,...**

Os códigos de produto para associar à imagem no momento do registro, separado por vírgulas.

Exigido: Não

**-B, --block-device-mapping mapping**

Define como dispositivos de blocos são expostos a uma instância dessa AMI, caso esse tipo de instância seja compatível com o dispositivo especificado.

Especifique uma lista separada por vírgulas de pares de valor-chave, nos quais cada chave é um nome virtual e cada valor é o nome do dispositivo correspondente. Os nomes virtuais incluem o seguinte:

- `ami` — o dispositivo do sistema de arquivos raiz, como visto pela instância
- `root` — o dispositivo do sistema de arquivos raiz, como visto pelo kernel

- swap — o dispositivo de troca, como visto pela instância
- ephemeralN — o enésimo volume de armazenamento de instâncias

Exigido: Não

**-a, --all**

Inclua todos os diretórios, incluindo aqueles em sistemas de arquivos montados remotamente.

Exigido: Não

**-e, --exclude directory1,directory2,...**

Uma lista de caminhos absolutos e arquivos no diretório para excluir a operação de pacotes. Esse parâmetro substitui a opção **--all**. Quando a exclusão for especificada, os diretórios subdiretórios listados com esse parâmetro não serão reunidos com o volume.

Exigido: Não

**-i, --include file1,file2,...**

Uma lista de arquivos a serem incluídos na operação de pacotes. Os arquivos especificados seriam excluídos da AMI, pois poderiam conter informações sigilosas.

Exigido: Não

**--no-filter**

Se especificado, não excluiremos os arquivos da AMI, pois eles podem conter informações sigilosas.

Exigido: Não

**-p, --prefix prefix**

O prefixo do nome dos arquivos de AMI em pacote.

Padrão: image

Exigido: Não

**-s, --size size**

O tamanho, em MB (1024 x 1024 bytes), do arquivo de imagem a ser criado. O tamanho máximo é de 10240 MB.

Padrão: 10240

Exigido: Não

**--[no-]inherit**

Indica se a imagem deve herdar metadados da instância (o padrão é herdar). O empacotamento falhará se você habilitar **--inherit**, mas os metadados de instância não estiverem acessíveis.

Exigido: Não

**-v, --volume volume**

O caminho absoluto até o volume montado, a partir do qual o pacote deve ser criado.

Padrão: O diretório de raiz (/)

Exigido: Não

**-P, --partition type**

Indica se a imagem do disco deve usar uma tabela de partição. Se você não especificar um tipo de tabela de partição, o padrão será o tipo usado no dispositivo de blocos do volume, se aplicável; caso contrário, o padrão é gpt.

Valores válidos: mbr | gpt | none

Exigido: Não

**-S, --script script**

Um script de personalização a ser sido executado logo antes do empacotamento. O script deve esperar um único argumento, o ponto de montagem do volume.

Exigido: Não

**--fstab path**

O caminho até fstab para empacotar na imagem. Se isso não estiver especificado, o Amazon EC2 empacotará /etc/fstab.

Exigido: Não

**--generate-fstab**

Empacote o volume usando um fstab fornecido pelo Amazon EC2.

Exigido: Não

**--grub-config**

O caminho para um arquivo alternativo de configuração do GRUB para empacotar na imagem. Por padrão, ec2-bundle-vol espera que /boot/grub/menu.lst ou /boot/grub/grub.conf exista na imagem clonada. Essa opção permite que você especifique um caminho para um arquivo alternativo de configuração do GRUB, que será então copiado para os padrões (se presente).

Exigido: Não

**--kernel kernel\_id**

Suspenso. Use [register-image](#) para configurar o kernel.

Exigido: Não

**--ramdiskramdisk\_id**

Suspenso. Use [register-image](#) para configurar o disco RAM, se necessário.

Exigido: Não

## Output

Mensagens de status que descrevem os estágios e o status do empacotamento.

## Example

Esse exemplo criar uma AMI empacotada ao comprimir, criptografar e assinar um snapshot do sistema de arquivos raiz da máquina local.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
Copying / into the image file /mnt/image...
Excluding:
  sys
  dev/shm
  proc
  dev/pts
  proc/sys/fs/binfmt_misc
  dev
  media
```

```
mnt
proc
sys
tmp/image
mnt/img-mnt
1+0 records in
1+0 records out
mke2fs 1.38 (30-Jun-2005)
warning: 256 blocks unused.

Splitting /mnt/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
...
Created image.part.22
Created image.part.23
Generating digests for each part...
Digests generated.
Creating bundle manifest...
Bundle Volume complete.
```

## ec2-delete-bundle

### Description

Exclui o pacote especificado do armazenamento Amazon S3. Após excluir um pacote, você não pode executar instâncias a partir da AMI correspondente.

### Syntax

```
ec2-delete-bundle -b bucket -a access_key_id -s secret_access_key [-t token]
[--url url] [--region region] [--sigv version] [-m path] [-p prefix] [--clear]
[--retry] [-y]
```

### Options

**-b, --bucket** *bucket*

O nome do bucket do Amazon S3 que contém a AMI empacotada, seguido por um prefixo de caminho opcional delimitado por '/'

Obrigatório: sim

**-a, --access-key** *access\_key\_id*

O ID da chave de acesso da AWS.

Obrigatório: sim

**-s, --secret-key** *secret\_access\_key*

A chave de acesso secreta da AWS.

Obrigatório: sim

**-t, --delegation-token** *token*

O token de delegação para repassar à solicitação da AWS. Para obter mais informações, consulte [Usar credenciais de segurança temporárias](#).

Obrigatório: Somente quando você usar credenciais temporárias de segurança.

Padrão: O valor da variável de ambiente `AWS_DELEGATION_TOKEN` (se definida).

**--region**

A região a ser usada na assinatura da solicitação.

Padrão: `us-east-1`

Obrigatório: Sim se estiver usando a assinatura versão 4

**--sigvversão**

A versão da assinatura a ser usada ao assinar a solicitação.

Valores válidos: `2 | 4`

Padrão: `4`

Exigido: Não

**-m, --manifestpath**

O caminho até o arquivo manifesto.

Obrigatório: Você deve especificar `--prefix` ou `--manifest`.

**-p, --prefix**

O prefixo do nome de arquivo da AMI empacotada. Forneça o prefixo inteiro. Por exemplo, se o prefixo for `image.img`, use `-p image.img`, não `-p image`

Obrigatório: Você deve especificar `--prefix` ou `--manifest`.

**--clear**

Exclui o bucket Amazon S3 se estiver vazio depois do pacote especificado.

Exigido: Não

**--retry**

Tenta novamente mais uma vez todos os erros de Amazon S3, até cinco vezes por operação.

Exigido: Não

**-y, --yes**

Pressupõe automaticamente que a resposta a todos os avisos é sim.

Exigido: Não

## Output

O Amazon EC2 exibe mensagens de status indicando os estágios e o status do processo de exclusão.

## Example

Este exemplo exclui um pacote do Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b DOC-EXAMPLE-BUCKET1 -a your_access_key_id -  
s your_secret_access_key  
Deleting files:  
DOC-EXAMPLE-BUCKET1/  
image.manifest.xml  
DOC-EXAMPLE-BUCKET1/  
image.part.00  
DOC-EXAMPLE-BUCKET1/  
image.part.01
```

```
DOC-EXAMPLE-BUCKET1/
image.part.02
DOC-EXAMPLE-BUCKET1/
image.part.03
DOC-EXAMPLE-BUCKET1/
image.part.04
DOC-EXAMPLE-BUCKET1/
image.part.05
DOC-EXAMPLE-BUCKET1/image.part.06
Continue? [y/n]
y
Deleted DOC-EXAMPLE-BUCKET1/image.manifest.xml
Deleted DOC-EXAMPLE-BUCKET1/image.part.00
Deleted DOC-EXAMPLE-BUCKET1/image.part.01
Deleted DOC-EXAMPLE-BUCKET1/image.part.02
Deleted DOC-EXAMPLE-BUCKET1/image.part.03
Deleted DOC-EXAMPLE-BUCKET1/image.part.04
Deleted DOC-EXAMPLE-BUCKET1/image.part.05
Deleted DOC-EXAMPLE-BUCKET1/image.part.06
ec2-delete-bundle complete.
```

## ec2-download-bundle

### Description

Faz download das AMIs do Linux com armazenamento de instâncias especificadas a partir do armazenamento do Amazon S3.

### Syntax

```
ec2-download-bundle -b bucket -a access_key_id -s secret_access_key -k path
[--url url] [--region region] [--sigv version] [-m file] [-p prefix] [-d
directory] [--retry]
```

### Options

**-b, --bucket** *bucket*

O nome do bucket Amazon S3 no qual o pacote está localizado, seguido por um prefixo de caminho opcional delimitado por '/'.

Obrigatório: sim

**-a, --access-key** *access\_key\_id*

O ID da chave de acesso da AWS.

Obrigatório: sim

**-s, --secret-key** *secret\_access\_key*

A chave de acesso secreta da AWS.

Obrigatório: sim

**-k, --privatekey** *path*

A chave privada usada para descriptografar o manifesto.

Obrigatório: sim

**--url** *url*

O URL do serviço Amazon S3.

Padrão: <https://s3.amazonaws.com/>

Exigido: Não

--region region

A região a ser usada na assinatura da solicitação.

Padrão: us-east-1

Obrigatório: Sim se estiver usando a assinatura versão 4

--sigv version

A versão da assinatura a ser usada ao assinar a solicitação.

Valores válidos: 2 | 4

Padrão: 4

Exigido: Não

-m, --manifest file

O nome do arquivo manifesto (sem o caminho). Recomendamos que você especifique o manifesto (-m) ou um prefixo (-p).

Exigido: Não

-p, --prefix prefix

O prefixo do nome dos arquivos de AMI em pacote.

Padrão: image

Exigido: Não

-d, --directory directory

O diretório no qual o pacote baixado é salvo. O diretório deve existir.

Padrão: O diretório de trabalho atual.

Exigido: Não

--retry

Tenta novamente mais uma vez todos os erros de Amazon S3, até cinco vezes por operação.

Exigido: Não

## Output

São exibidas as mensagens de status que indicam os vários estágios do processo de download.

## Example

Este exemplo cria o diretório bundled (usando o comando Linux mkdir) e faz download do pacote do bucket **DOC-EXAMPLE-BUCKET1** do Amazon S3.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name
-m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from DOC-EXAMPLE-BUCKET1 to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/
image.part.00 ...
Downloaded image.part.00 from DOC-EXAMPLE-BUCKET1
```

```
Downloading part image.part.01 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/  
image.part.01 ...  
Downloaded image.part.01 from DOC-EXAMPLE-BUCKET1  
Downloading part image.part.02 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/  
image.part.02 ...  
Downloaded image.part.02 from DOC-EXAMPLE-BUCKET1  
Downloading part image.part.03 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/  
image.part.03 ...  
Downloaded image.part.03 from DOC-EXAMPLE-BUCKET1  
Downloading part image.part.04 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/  
image.part.04 ...  
Downloaded image.part.04 from DOC-EXAMPLE-BUCKET1  
Downloading part image.part.05 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/  
image.part.05 ...  
Downloaded image.part.05 from DOC-EXAMPLE-BUCKET1  
Downloading part image.part.06 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to mybundle/  
image.part.06 ...  
Downloaded image.part.06 from DOC-EXAMPLE-BUCKET1
```

## ec2-migrate-manifest

### Description

Modifica uma AMI em Linux com armazenamento de instâncias (por exemplo, seu certificado, kernel e disco RAM), de forma que suporte uma região diferente.

### Syntax

```
ec2-migrate-manifest -c path -k path -m path {(-a access_key_id -s  
  secret_access_key --region region) | (--no-mapping)} [--ec2cert ec2_cert_path]  
  [--kernel kernel_id] [--ramdisk ramdisk_id]
```

### Options

**-c, --cert *path***

O arquivo de certificado de chave pública RSA codificado por PEM do usuário.

Obrigatório: sim

**-k, --privatekey *path***

O caminho até o arquivo de chaves RSA codificado por PEM do usuário.

Obrigatório: sim

**--manifest *path***

O caminho até o arquivo manifesto.

Obrigatório: sim

**-a, --access-key *access\_key\_id***

O ID da chave de acesso da AWS.

Obrigatório: Obrigatório se estiver usando o mapeamento automático.

**-s, --secret-key *secret\_access\_key***

A chave de acesso secreta da AWS.

Obrigatório: Obrigatório se estiver usando o mapeamento automático.

**--region *region***

A região a pesquisar no arquivo de mapeamento.

Obrigatório: Obrigatório se estiver usando o mapeamento automático.

--no-mapping

Desabilita o mapeamento automático de kernels e discos RAM.

Durante a migração, o Amazon EC2 substitui o kernel e o disco RAM no arquivo manifesto por um kernel e disco RAM projetados para a região de destino. A menos que o parâmetro --no-mapping seja fornecido, `ec2-migrate-bundle` poderá usar as operações `DescribeRegions` e `DescribeImages` para executar mapeamentos automatizados.

Obrigatório: Obrigatório se não fornecer as opções `-a`, `-s` e `--region` usadas para mapeamento automático.

--ec2cert path

O caminho até o certificado de chave pública X.509 do Amazon EC2 usado para criptografar o manifesto da imagem.

As regiões `us-gov-west-1` e `cn-north-1` usam um certificado de chave pública não padrão e o caminho para esse certificado deve ser especificado com essa opção. O caminho para o certificado varia de acordo com o método de instalação das ferramentas da AMI. Para o Amazon Linux, os certificados estão localizados em `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Se você tiver instalado as ferramentas da AMI do arquivo ZIP em [Configurar as ferramentas da AMI \(p. 114\)](#), os certificados estarão localizados em `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Obrigatório: apenas para as regiões `us-gov-west-1` e `cn-north-1`.

--kernel kernel\_id

O ID do kernel para selecionar.

Important

Recomendamos que você use PV-GRUB em vez de kernels e discos RAM. Para obter mais informações, consulte [Enabling Your Own Linux Kernels \(p. 191\)](#).

Exigido: Não

--ramdisk ramdisk\_id

O ID do disco RAM para selecionar.

Important

Recomendamos que você use PV-GRUB em vez de kernels e discos RAM. Para obter mais informações, consulte [Enabling Your Own Linux Kernels \(p. 191\)](#).

Exigido: Não

**Output**

Mensagens de status que descrevem os estágios e o status do processo de empacotamento.

**Example**

Este exemplo copia a AMI especificada no manifesto `my-ami.manifest.xml` dos EUA para a União Europeia.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CL0.pem --privatekey pk-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CL0.pem --region eu-west-1
```

```
Backing up manifest...
```

```
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

## ec2-unbundle

### Description

Recria o pacote a partir de uma AMI em Linux com armazenamento de instâncias.

### Syntax

```
ec2-unbundle -k path -m path [-s source_directory] [-d destination_directory]
```

### Options

**-k, --privatekey path**

O caminho para seu arquivo de chave RSA codificado por PEM.

Obrigatório: sim

**-m, --manifest path**

O caminho até o arquivo manifesto.

Obrigatório: sim

**-s, --source source\_directory**

O diretório que contém o pacote.

Padrão: O diretório atual.

Exigido: Não

**-d, --destination destination\_directory**

O diretório no qual o pacote da AMI deve ser desfeito. O diretório de destino deve existir.

Padrão: O diretório atual.

Exigido: Não

### Example

Este exemplo de Linux e UNIX desfaz o pacote da AMI especificado no arquivo `image.manifest.xml`.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s
mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

## Output

São exibidas mensagens de status indicando os vários estágios do processo de desempacotamento.

## ec2-upload-bundle

### Description

Faz upload do pacote de uma AMI do Linux com armazenamento de instâncias para o Amazon S3 e define as ACLs apropriadas nos objetos carregados. Para obter mais informações, consulte [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#).

## Syntax

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t token] -m path [--url url] [--region region] [--sigv version] [--acl acl] [-d directory] [--part part] [--retry] [--skipmanifest]
```

## Options

**-b, --bucket** *bucket*

O nome do bucket Amazon S3 no qual armazenar o pacote, seguido por um prefixo de caminho opcional delimitado por '/'. Se o bucket não existir, ele será criado se o nome do bucket estiver disponível.

Obrigatório: sim

**-a, --access-key** *access\_key\_id*

Seu ID de chave de acesso da AWS.

Obrigatório: sim

**-s, --secret-key** *secret\_access\_key*

Sua chave de acesso secreta da AWS.

Obrigatório: sim

**-t, --delegation-token** *token*

O token de delegação para repassar à solicitação da AWS. Para obter mais informações, consulte [Usar credenciais de segurança temporárias](#).

Obrigatório: Somente quando você usar credenciais temporárias de segurança.

Padrão: O valor da variável de ambiente `AWS_DELEGATION_TOKEN` (se definida).

**-m, --manifest** *path*

O caminho até o arquivo manifesto. O arquivo manifesto é criado durante o processo de empacotamento e pode ser localizado no diretório que contém o pacote.

Obrigatório: sim

**--url** *url*

Suspenso. Use a opção **--region** a menos que seu bucket esteja restrito ao local EU (e não eu-west-1). A marca **--location** é uma única forma de destinar essa restrição específica de local.

O URL do serviço de endpoint do Amazon S3.

Padrão: <https://s3.amazonaws.com/>

Exigido: Não

**--region** *region*

A região a ser usada na assinatura da solicitação para o bucket do S3 de destino.

- Se o bucket não existir e você não especificar uma região, a ferramenta criará o bucket sem uma restrição de local (em us-east-1).
- Se o bucket não existir e você especificar uma região, a ferramenta criará o bucket na região especificada.
- Se o bucket existir e você não especificar uma região, a ferramenta usará o local do bucket.

- Se o bucket existir e você especificar `us-east-1` como região, a ferramenta usará o local real do bucket sem nenhuma mensagem de erro e todos os arquivos correspondentes serão substituídos.
- Se o bucket existir e você especificar uma região (além de `us-east-1`) que não corresponde ao local real do bucket, a ferramenta sairá com um erro.

Se seu bucket estiver restrito ao local EU (e não eu-west-1), use a marca `--location`. A marca `--location` é uma única forma de destinar essa restrição específica de local.

Padrão: `us-east-1`

Obrigatório: Sim se estiver usando a assinatura versão 4  
`--sigv version`

A versão da assinatura a ser usada ao assinar a solicitação.

Valores válidos: 2 | 4

Padrão: 4

Exigido: Não

`--acl acl`

A política de lista de controle de acesso da imagem empacotada.

Valores válidos: `public-read` | `aws-exec-read`

Padrão: `aws-exec-read`

Exigido: Não

`-d, --directory directory`

O diretório que contém as partes da AMI empacotadas.

Padrão: O diretório que contém o arquivo manifesto (veja a opção `-m`).

Exigido: Não

`--part part`

Inicia a transferência da parte especificada e de todas as partes subsequentes. Por exemplo, `--part 04`.

Exigido: Não

`--retry`

Tenta novamente mais uma vez todos os erros de Amazon S3, até cinco vezes por operação.

Exigido: Não

`--skipmanifest`

Não faz upload do manifesto.

Exigido: Não

`--location location`

Suspensão. Use a opção `--region`, a menos que seu bucket esteja restrito ao local EU (e não eu-west-1). A marca `--location` é uma única forma de destinar essa restrição específica de local.

A restrição do local do bucket Amazon S3 de destino. Se o bucket existir e você especificar um local que não corresponde ao local real do bucket, a ferramenta sairá com um erro. Se o bucket existir e

você não especificar um local, a ferramenta usará o local do bucket. Se o bucket não existir e você especificar um local, a ferramenta criará o bucket no local especificado. Se o bucket não existir e você não especificar um local, a ferramenta criará o bucket sem uma restrição de local (em `us-east-1`).

Padrão: se `--region` for especificado, o local será definido para essa região especificada. Se `--region` não for especificado, o local padrão será `us-east-1`.

Exigido: Não

## Output

O Amazon EC2 exibe mensagens de status que indicam os estágios e o status do processo de upload.

### Example

Esse exemplo faz uploads do pacote especificado pelo manifesto `image.manifest.xml`.

```
[ec2-user ~]$ ec2-upload-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name -m image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket DOC-EXAMPLE-BUCKET1 ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

## Opções comuns de ferramentas da AMI

A maioria das ferramentas da AMI aceita os parâmetros opcionais a seguir.

`--help, -h`

Exibe a mensagem de ajuda.

`--version`

Exibe a notificação de versão e direitos autorais.

`--manual`

Exibe a entrada manual.

`--batch`

Executa no modo em lote, suprimindo prompts interativos.

`--debug`

Exibe informações que podem ser úteis ao resolver problemas.

## 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 Linux baseada em Amazon EBS \(p. 107\)](#).

### Tópicos

- [Permissões para copiar uma AMI com armazenamento de instâncias \(p. 144\)](#)
- [Copiar um AMI \(p. 145\)](#)
- [Parar uma operação de cópia de AMI pendente \(p. 146\)](#)
- [Cópia entre regiões \(p. 147\)](#)
- [Cópia entre contas \(p. 148\)](#)
- [Criptografar e copiar \(p. 148\)](#)

## 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`, `s3:GetObject`, `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": "s3:GetObject",  
            "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 Linux baseada em Amazon EBS \(p. 107\)](#) e [Localização de 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 \(p. 147\)](#).
  - 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 recriptografá-los usando uma chave diferente. Se você tiver ativado a [criptografia por padrão \(p. 1421\)](#), a opção Encryption (Criptografia) será configurada e não poderá ser desconfigurada no console do snapshot. Para obter mais informações, consulte [Criptografar e copiar \(p. 148\)](#).
  - 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 \(p. 3\)](#).

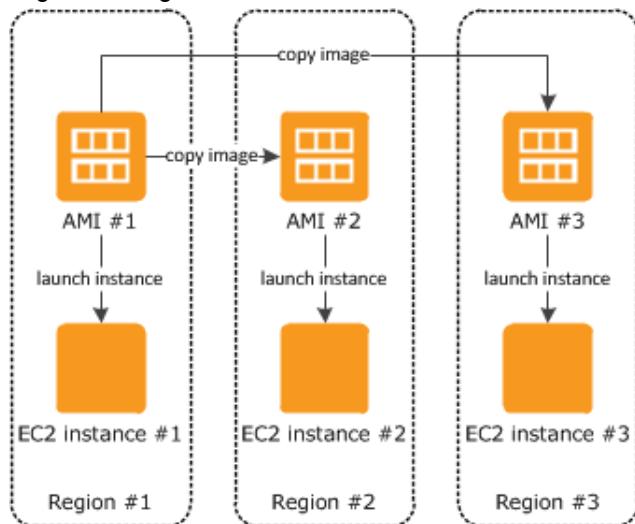
- [deregister-image](#) (AWS CLI)
- [Unregister-EC2Image](#) (AWS Tools for Windows PowerShell)

## 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.
- Não é possível copiar uma AMI paravirtual (PV) em uma região que não oferece suporte a AMIs PV. Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#).

## 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 \(p. 96\)](#).

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, seu 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 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.

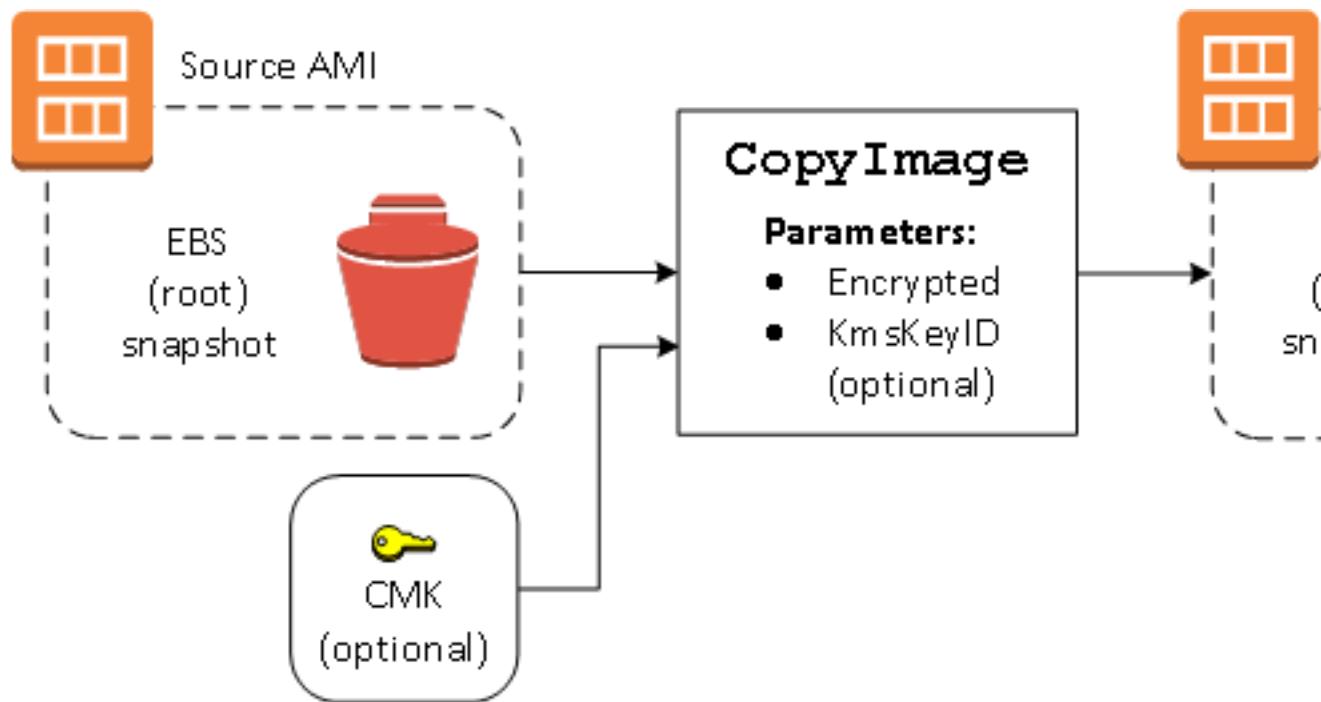
Se você especificar parâmetros de criptografia enquanto copia uma AMI, poderá criptografar seus snapshots de suporte ou criptografá-los novamente. O exemplo a seguir mostra um caso não padrão que fornece parâmetros de criptografia à ação `CopyImage` para alterar o estado de criptografia da AMI de destino.

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 \(p. 1421\)](#) 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 \(p. 163\)](#).

## 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 partições da AWS ou regiões da AWS, incluindo, entre outros, quaisquer regulamentos governamentais aplicáveis e requisitos de residência de dados.

**Tópicos**

- [Casos de uso \(p. 150\)](#)
- [Como as APIs de armazenamento e restauração da AMI funcionam \(p. 151\)](#)
- [Limitations \(p. 153\)](#)
- [Costs \(p. 153\)](#)
- [Proteger suas AMIs \(p. 153\)](#)
- [Permissões para armazenar e restaurar AMIs usando o S3 \(p. 153\)](#)
- [Trabalhar com o armazenamento da AMI e restaurar APIs \(p. 154\)](#)

## 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 \(p. 150\)](#)
- [Fazer cópias de arquivamento de AMIs \(p. 151\)](#)

## 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 \(p. 154\)](#).
- 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 \(p. 155\)](#).
- 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 partições 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 partições, 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 \(p. 155\)](#).
- 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 \(p. 154\)](#).

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 \(p. 151\)](#)
- [DescribeStoreImageTasks \(p. 152\)](#)
- [CreateRestoreImageTask \(p. 152\)](#)

### CreateStoreImageTask

A API [CreateStoreImageTask \(p. 154\)](#) 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 \(p. 155\)](#).

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 \(p. 155\)](#) 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 [CreateRestoreImageTask \(p. 155\)](#) inicia uma tarefa que restaura uma AMI de um objeto do S3 que foi criado anteriormente usando uma solicitação [CreateStoreImageTask \(p. 154\)](#).

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 \(p. 154\)](#) : 600 GB de trabalho de armazenamento (dados de snapshots) em andamento.
- Cota em solicitações de [imagem de restauração \(p. 155\)](#) : 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 \(p. 154\)](#)
- [Descrever o andamento de uma tarefa de armazenamento de AMI \(p. 155\)](#)
- [Restaurar uma AMI de um bucket do S3 \(p. 155\)](#)

### 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"  
}
```

## Defasá 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 \(p. 159\)](#) dela.

Depois que uma AMI estiver defasada:

- Para usuários de AMI, a AMI defasada não aparece nas chamadas de API [DescribelImages](#), 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 [DescribelImages](#).
- 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 defasgar 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 \(p. 1372\)](#).

#### Tópicos

- [Costs \(p. 156\)](#)
- [Limitations \(p. 153\)](#)
- [Defasgar uma AMI \(p. 156\)](#)
- [Descrever AMIs defasadas \(p. 157\)](#)
- [Cancelar a defasagem de uma AMI \(p. 158\)](#)

## Costs

Quando você defasgar 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 \(p. 159\)](#) dela.

## Limitations

- Para defasgar uma AMI, é necessário ser o proprietário da AMI.
- Não é possível usar o console do EC2 para defasgar uma AMI ou cancelar a defasagem de uma AMI.

## Defasgar uma AMI

Você pode defasgar uma AMI em uma data e hora específicas. É necessário ser o proprietário da AMI para executar esse procedimento.

Para defasgar 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",  
            "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"  
}
```

## Cancelar AMI do Linux

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

Quando você cancelar o registro de uma AMI, isso não afetará nenhuma instância que você já tenha executado pela AMI. Os custos de utilização continuarão a ser cobrados dessas instâncias. Portanto, se você tiver terminado de trabalhar com essas instâncias, deverá encerrá-las.

O procedimento que usará para liberar sua AMI dependerá de se ela é baseada em Amazon EBS ou armazenamento de instâncias. Para obter mais informações, consulte [Determinar o tipo de dispositivo raiz da AMI \(p. 76\)](#).

### Note

Uma AMI deve ser de propriedade da sua conta para cancelar o registro.

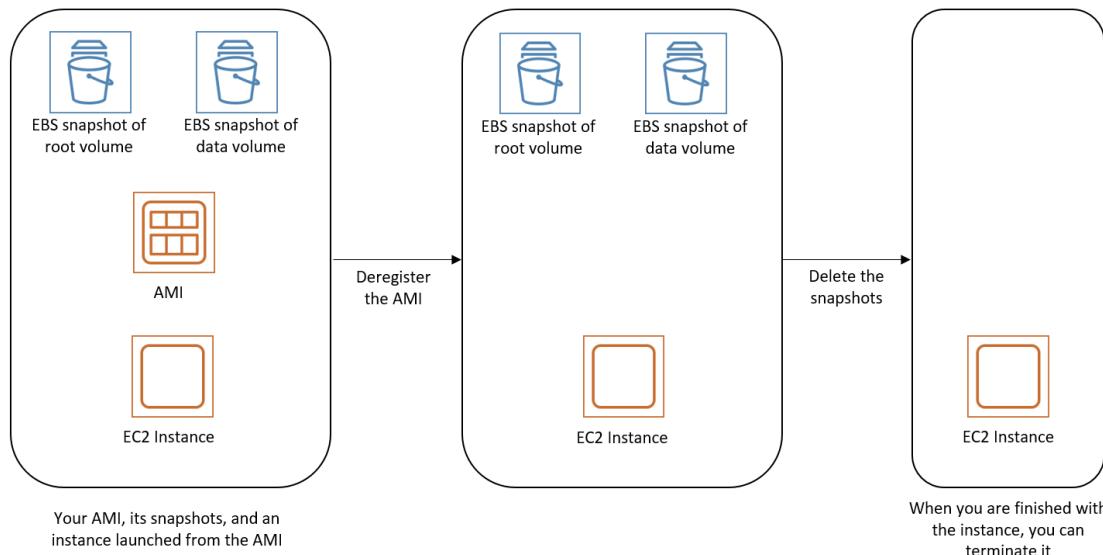
### Tópicos

- [Limpar sua AMI com armazenamento de Amazon EBS \(p. 159\)](#)
- [Limpar sua AMI com armazenamento de instâncias \(p. 162\)](#)

## Limpar sua AMI com armazenamento de Amazon EBS

Quando você cancelar o registro de uma AMI baseada em Amazon EBS, isso não afetará os snapshots criados para o volume da instância durante o processo de criação da AMI. Você continuará a acumular custos de armazenamento para os snapshots. Portanto, se você tiver terminado de usar o snapshot, exclua-os.

O diagrama a seguir ilustra o processo para limpar a AMI com Amazon EBS.



Você pode usar um dos métodos a seguir para limpar sua AMI baseada em Amazon EBS.

## New console

Para limpar sua AMI baseada em Amazon EBS pelo console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Cancele o registro da AMI
  - a. No painel de navegação, selecione AMIs.
  - b. Selecione a AMI cujo registro deve ser cancelado e anote seu ID — isso pode ajudar você a encontrar os snapshots a serem excluídos na próxima etapa.
  - c. Escolha Actions (Ações) e, em seguida, Deregister (Cancelar o registro). Quando solicitada a confirmação, selecione Continue (Continuar).

### Note

A remoção da AMI da lista pelo console pode demorar alguns minutos. Escolha Refresh (Atualizar) para atualizar o status.

3. Exclua snapshots que não sejam mais necessários
  - a. No painel de navegação, selecione Snapshots.
  - b. Selecione um snapshot a ser excluído (procure o ID da AMI na etapa anterior da coluna Description (Descrição)).
  - c. Escolha Actions (Ações) e, em seguida, escolha Excluir. Quando a confirmação for solicitada, escolha Yes, Delete (Sim, excluir).
4. Encerrar instâncias (opcional)

(Opcional) Se você terminou de trabalhar com uma instância executada pela AMI, encerre-a.

  - a. No painel de navegação, selecione Instances (Instâncias) e selecione a instância a ser encerrada.
  - b. Escolha Actions (Ações), depois Instance state (Estado da instância) e escolha Terminate instance (Encerrar instância). Quando a confirmação for solicitada, escolha Terminate (Encerrar).

### Note

Talvez seja necessário rolar para baixo, para visualizar alguns dos itens do menu Actions (Ações).

## Old console

Para limpar sua AMI baseada em Amazon EBS pelo console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Cancele o registro da AMI
  - a. No painel de navegação, selecione AMIs.
  - b. Selecione a AMI cujo registro deve ser cancelado e anote seu ID — isso pode ajudar você a encontrar os snapshots a serem excluídos na próxima etapa.
  - c. Escolha Actions (Ações) e, em seguida, Deregister (Cancelar o registro). Quando solicitada a confirmação, selecione Continue (Continuar).

### Note

A remoção do AMI da lista pelo console pode demorar alguns minutos. Escolha Refresh (Atualizar) para atualizar o status.

3. Exclua snapshots que não sejam mais necessários
  - a. No painel de navegação, selecione Snapshots.
  - b. Selecione um snapshot a ser excluído (procure o ID da AMI na etapa anterior da coluna Description (Descrição)).
  - c. Escolha Ações e, em seguida, escolha Excluir. Quando a confirmação for solicitada, escolha Yes, Delete (Sim, excluir).
4. Encerrar instâncias (opcional)

(Opcional) Se você terminou de trabalhar com uma instância executada pela AMI, encerre-a.

  - a. No painel de navegação, selecione Instances (Instâncias) e selecione a instância a ser encerrada.
  - b. Escolha Actions (Ações), depois Instance State (Estado da instância) e escolha Terminate (Encerrar). Quando a confirmação for solicitada, escolha Sim, encerrar.

## AWS CLI

Siga estes passos para limpar a AMI baseada no Amazon EBS usando a AWS CLI

1. Cancele o registro da AMI

Cancele o registro da AMI usando o comando [deregister-image](#):

```
aws ec2 deregister-image --image-id ami-12345678
```

2. Exclua snapshots que não sejam mais necessários

Exclua os snapshots que não forem mais necessários usando o comando [delete-snapshot](#):

```
aws ec2 delete-snapshot --snapshot-id snap-1234567890abcdef0
```

3. Encerrar instâncias (opcional)

Se você terminou de trabalhar com uma instância executada pela AMI, encerre-a usando o comando [terminate-instances](#):

```
aws ec2 terminate-instances --instance-ids i-12345678
```

## PowerShell

Siga estes passos para limpar a AMI baseada no Amazon EBS usando a AWS Tools for Windows PowerShell

1. Cancele o registro da AMI

Cancele o registro da AMI usando o cmdlet [Unregister-EC2Image](#):

```
Unregister-EC2Image -ImageId ami-12345678
```

2. Exclua snapshots que não sejam mais necessários

Exclua os snapshots que não forem mais necessários usando o cmdlet [Remove-EC2Snapshot](#):

```
Remove-EC2Snapshot -SnapshotId snap-12345678
```

3. Encerrar instâncias (opcional)

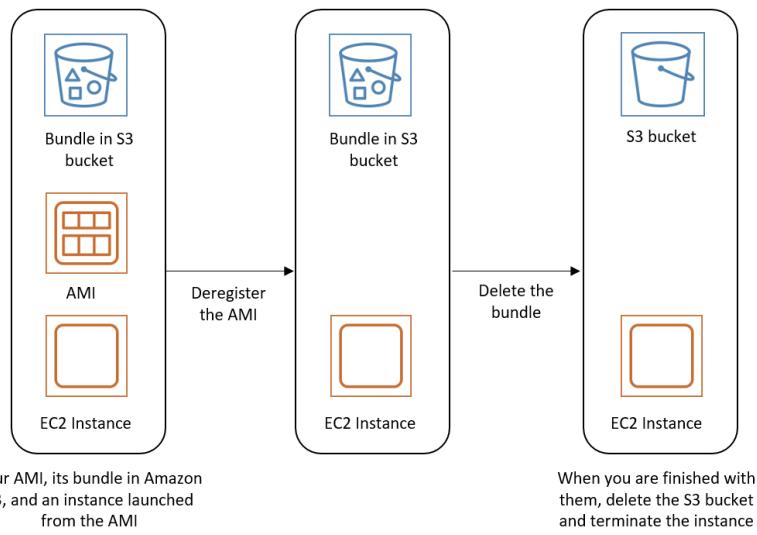
Se você terminar com uma instância executada da AMI, você poderá encerrá-la usando o cmdlet [Remove-EC2Instance](#):

```
Remove-EC2Instance -InstanceId i-12345678
```

## Limpar sua AMI com armazenamento de instâncias

Quando você cancelar o registro de uma AMI com armazenamento de instâncias, isso não afetará os arquivos que você carregou no Amazon S3 quando criar a AMI. De você continuarão a ser cobrados custos de utilização desses arquivos no Amazon S3. Portanto, se você tiver terminado de trabalhar com esses arquivos, exclua-os.

O diagrama a seguir ilustra o processo para limpar sua AMI com armazenamento de instâncias.



### Para limpar sua AMI com armazenamento de instâncias

1. Cancele o registro da AMI usando o comando [deregister-image](#), da seguinte forma.

```
aws ec2 deregister-image --image-id ami_id
```

2. Exclua o pacote no Amazon S3 usando o comando [ec2-delete-bundle](#) (p. 134) (ferramentas de AMI) da seguinte forma.

```
ec2-delete-bundle -b myawsbucket/myami -a your_access_key_id -s your_secret_access_key -p image
```

3. (Opcional) Se você tiver terminado de trabalhar com uma instância executada pela AMI, poderá encerrá-la usando o comando [terminate-instances](#) da seguinte forma.

```
aws ec2 terminate-instances --instance-ids instance_id
```

4. (Opcional) Se você tiver terminado de usar o bucket Amazon S3 para o qual carregou o pacote, pode excluí-lo. Para excluir um bucket do Amazon S3, abra o console do Amazon S3, selecione o bucket, escolha Actions (Ações) e selecione Delete (Excluir).

## 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 \(p. 1359\)](#).

## 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 \(p. 92\)](#).

Tópicos de criptografia em AMIs com EBS

- [Cenários de execução de instância \(p. 163\)](#)
- [Cenários de cópia de imagem \(p. 166\)](#)

## 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 \(p. 1421\)](#) 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.

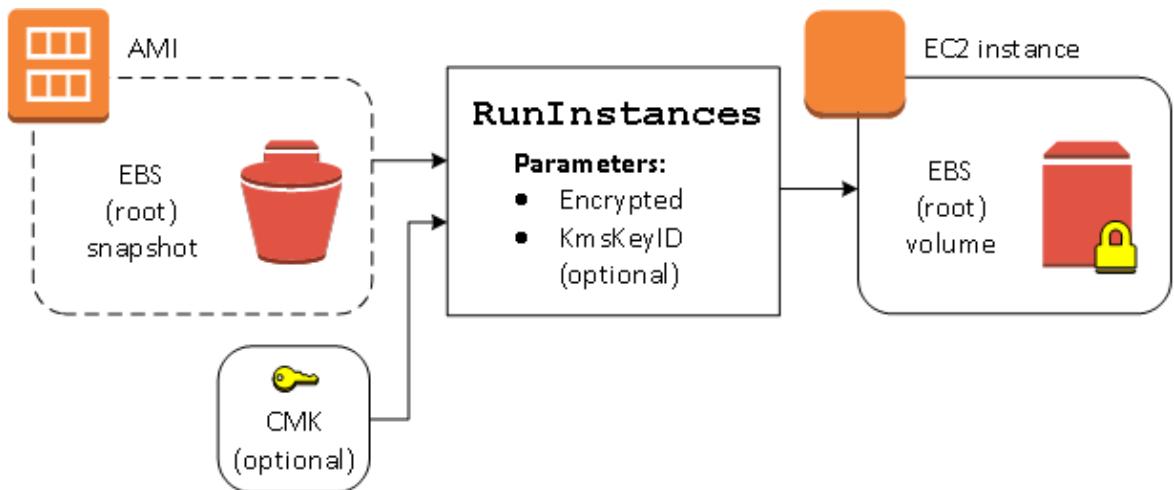
Enviar um `KmsKeyId` sem também configurar o parâmetro `Encrypted` resulta em um erro.

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 \(p. 509\)](#).

## Criptografar um volume durante a execução

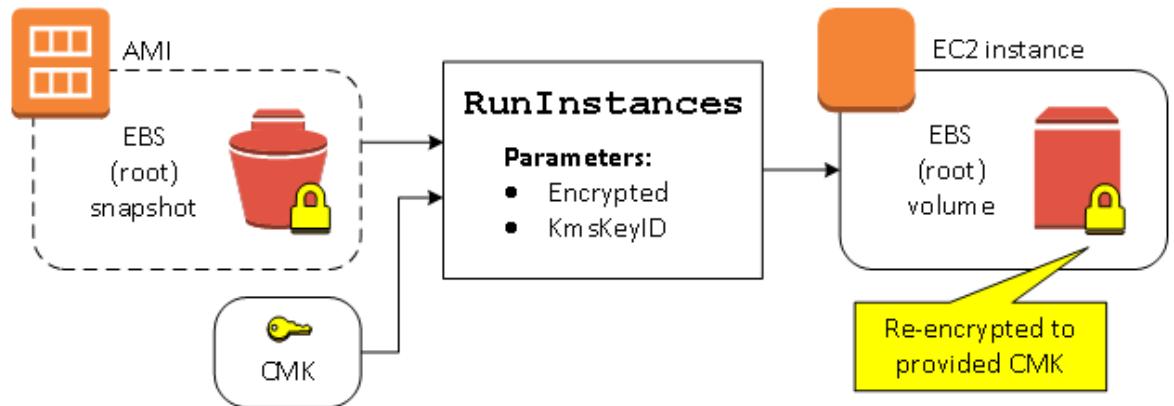
Neste exemplo, uma AMI baseada em um snapshot não criptografado é usada para executar uma instância do EC2 com um volume não criptografado do EBS.



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

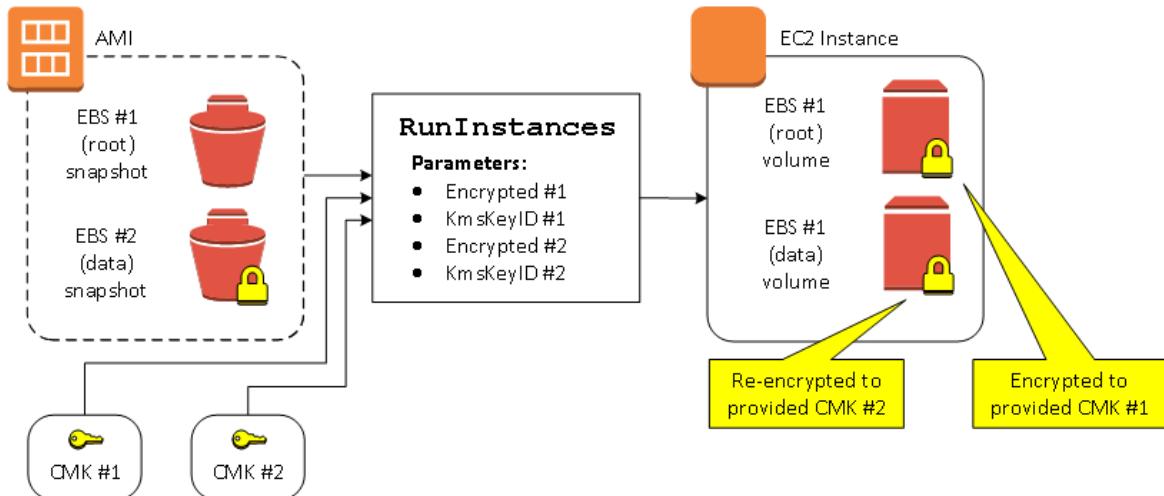
Neste exemplo, uma AMI baseada em um snapshot criptografado é usada para executar uma instância do EC2 com um volume do EBS criptografado por uma nova Chave do KMS.



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.

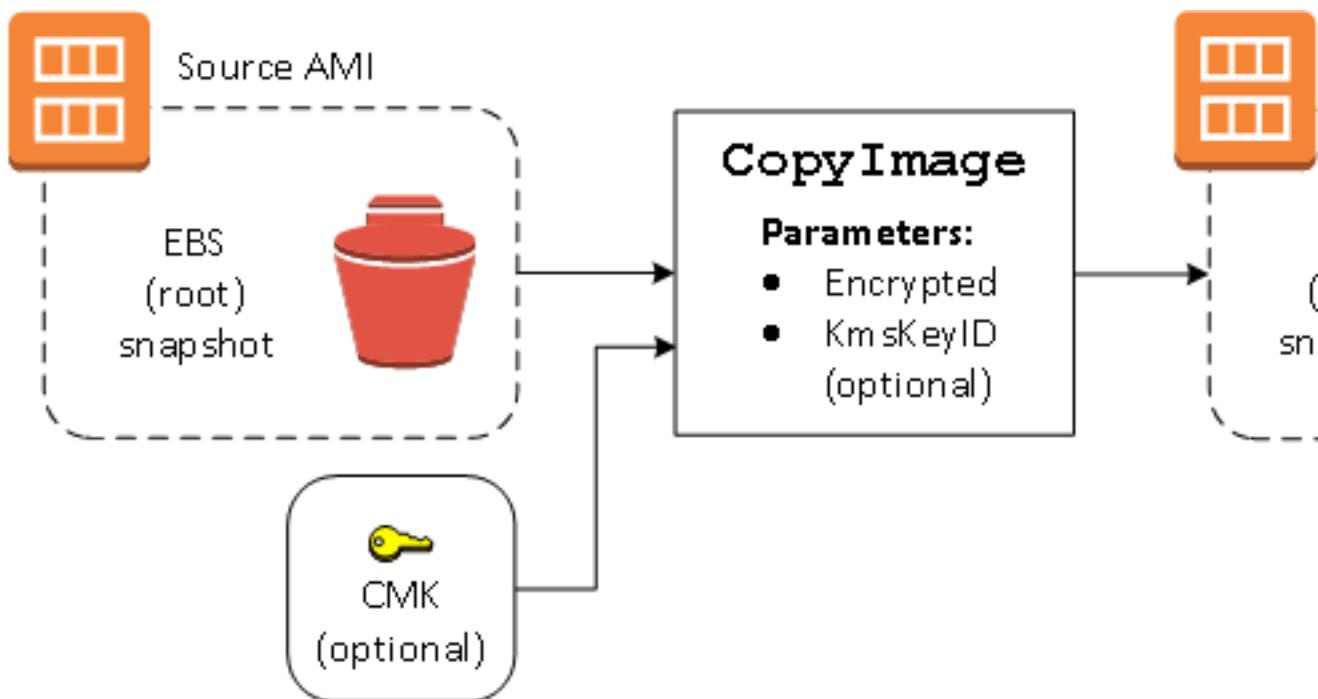
Para obter instruções detalhadas usando o console, consulte [Copiar um AMI \(p. 144\)](#).

## 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 \(p. 1421\)](#) 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 \(p. 169\)](#)

- Localizando detalhes de faturamento e uso da AMI (p. 170)
- Verificar cobranças da AMI em sua fatura (p. 172)

## 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 Padrão 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.

## Amazon Linux

O Amazon Linux é fornecido pela Amazon Web Services (AWS). Ele foi criado para fornecer um ambiente de execução estável, seguro e de alta performance para aplicações em execução no Amazon EC2. Ele também inclui vários pacotes que permitem a fácil integração com a AWS, incluindo ferramentas de configuração de execução e muitas bibliotecas e ferramentas populares da AWS. O AWS fornece atualizações constantes de segurança e manutenção para todas as instâncias que executam o Amazon Linux. Muitas aplicações desenvolvidas no CentOS (e distribuições similares) são executadas no Amazon Linux.

### Tópicos

- [Disponibilidade do Amazon Linux \(p. 173\)](#)
- [Conectar-se a uma instância do Amazon Linux \(p. 173\)](#)
- [Identificar imagens do Amazon Linux \(p. 173\)](#)
- [AWSFerramentas da linha de comando da \(p. 174\)](#)
- [Repositório de pacotes \(p. 175\)](#)
- [Biblioteca de extras \(Amazon Linux 2\) \(p. 178\)](#)
- [Acessar pacotes de origem para referência \(p. 178\)](#)
- [cloud-init \(p. 179\)](#)
- [Assinar notificações do Amazon Linux \(p. 180\)](#)
- [Executar o Amazon Linux 2 como máquina virtual no local \(p. 182\)](#)

- [Kernel Live Patching no Amazon Linux 2 \(p. 186\)](#)

## Disponibilidade do Amazon Linux

A AWS fornece o Amazon Linux 2 e a Amazon Linux AMI. Se você estiver migrando de outra distribuição do Linux para o Amazon Linux, recomendamos migrar para o Amazon Linux 2.

A última versão da AMI do Amazon Linux, 2018.03, chegou ao final do suporte padrão em 31 de dezembro de 2020. Para obter mais informações, consulte a seguinte postagem no blog: [Amazon Linux AMI end of life](#). Se atualmente você estiver usando o Amazon Linux AMI, recomendamos migrar para o Amazon Linux 2. Para migrar para o Amazon Linux 2, inicie uma instância ou crie uma máquina virtual usando a imagem atual do Amazon Linux 2. Instale suas aplicações, além dos pacotes necessários. Teste a aplicação e faça todas as alterações necessárias para que ela seja executada no Amazon Linux 2.

Para obter mais informações, consulte [Amazon Linux 2](#) e [Amazon Linux AMI](#). Para obter imagens de contêiner do Docker do Amazon Linux, consulte [amazonlinux](#) no Docker Hub.

## Conectar-se a uma instância do Amazon Linux

O Amazon Linux não permite SSH de raiz remota por padrão. Além disso, a autenticação da senha é desabilitada para evitar ataques de força bruta em senhas. Para permitir logins SSH a uma instância Amazon Linux, você deve fornecer seu par de chaves à instância na execução. Você também deve definir o security group usado para executar sua instância para permitir acesso SSH. Por padrão, a única conta que pode fazer login remotamente usando SSH é o ec2-user; essa conta também tem privilégios sudo. Se você habilitar o login de raiz remoto, saiba que é menos seguro do que recorrer a pares de chaves e um usuário secundário.

## Identificar imagens do Amazon Linux

Cada imagem contém um arquivo `/etc/image-id` exclusivo que a identifica. Esse arquivo contém as seguintes informações sobre a imagem:

- `image_name`, `image_version`, `image_arch` — Valores da receita de compilação que a Amazon usou para criar a imagem.
- `image_stamp` — Valor hexadecimal aleatório exclusivo gerado durante a criação da imagem.
- `image_date` — o horário UTC da criação da imagem, no formato AAAAMMDDhhmmss
- `recipe_name`, `recipe_id` — O nome e o ID da receita de compilação que a Amazon usou para criar a imagem.

O Amazon Linux contém um arquivo `/etc/system-release` que especifica a versão atual que está instalada. Esse arquivo é atualizado com o yum e faz parte do RPM `system-release`.

O Amazon Linux também contém uma versão legível por máquina do `/etc/system-release` que acompanha a especificação de CPE; consulte `/etc/system-release-cpe`.

## Amazon Linux 2

O exemplo a seguir é do `/etc/image-id` para a versão atual do Amazon Linux 2:

```
[ec2-user ~]$ cat /etc/image-id
image_name="amzn2-ami-hvm"
image_version="2"
image_arch="x86_64"
```

```
image_file="amzn2-ami-hvm-2.0.20180810-x86_64.xfs.gpt"
image_stamp="8008-2abd"
image_date="20180811020321"
recipe_name="amzn2 ami"
recipe_id="c652686a-2415-9819-65fb-4dee-9792-289d-1e2846bd"
```

O exemplo a seguir é do /etc/system-release para a versão atual do Amazon Linux 2:

```
[ec2-user ~]$ cat /etc/system-release
Amazon Linux 2
```

Veja a seguir um exemplo de /etc/os-release para o Amazon Linux 2:

```
[ec2-user ~]$ cat /etc/os-release
NAME="Amazon Linux"
VERSION="2"
ID="amzn"
ID_LIKE="centos rhel fedora"
VERSION_ID="2"
PRETTY_NAME="Amazon Linux 2"
ANSI_COLOR="0;33"
CPE_NAME="cpe:2.3:o:amazon:amazon_linux:2"
HOME_URL="https://amazonlinux.com/"
```

## AMI do Amazon Linux

O exemplo a seguir é do /etc/image-id para a versão atual do Amazon Linux AMI:

```
[ec2-user ~]$ cat /etc/image-id
image_name="amzn-ami-hvm"
image_version="2018.03"
image_arch="x86_64"
image_file="amzn-ami-hvm-2018.03.0.20180811-x86_64.ext4.gpt"
image_stamp="cc81-f2f3"
image_date="20180811012746"
recipe_name="amzn ami"
recipe_id="5b283820-dc60-a7ea-d436-39fa-439f-02ea-5c802dbd"
```

O exemplo a seguir é do /etc/system-release para a versão atual do Amazon Linux AMI:

```
[ec2-user ~]$ cat /etc/system-release
Amazon Linux AMI release 2018.03
```

## AWSFerramentas da linha de comando da

As ferramentas de linha de comando a seguir para integração e uso da AWS estão incluídas no Amazon Linux AMI ou nos repositórios padrão do Amazon Linux 2. Para obter a lista completa de pacotes, no Amazon Linux AMI, consulte [Pacotes do Amazon Linux AMI 2017.09](#).

- aws-amitools-ec2
- aws-apitools-as
- aws-apitools-cfn
- aws-apitools-elb
- aws-apitools-mon
- aws-cfn-bootstrap

- aws-cli

O Amazon Linux 2 e as versões mínimas do Amazon Linux (`amzn-ami-minimal-*` e `amzn2-ami-minimal-*`) nem sempre contêm todos esses pacotes; contudo, é possível instalá-los usando os repositórios padrão por meio do seguinte comando:

```
[ec2-user ~]$ sudo yum install -y package_name
```

Para instâncias executadas usando funções do IAM, um script simples foi incluído para preparar `AWS_CREDENTIAL_FILE`, `JAVA_HOME`, `AWS_PATH`, `PATH` e variáveis de ambiente específicas do produto depois que um arquivo de credenciais foi instalado para simplificar a configuração dessas ferramentas.

Além disso, para permitir a instalação de várias versões das ferramentas de API e AMI, colocamos links simbólicos para as versões desejadas dessas ferramentas em `/opt/aws`, como descrito aqui:

`/opt/aws/bin`

Links simbólicos para os diretórios `/bin` em cada um dos diretórios de ferramentas instaladas.

`/opt/aws/{apitools|amitools}`

Os produtos são instalados em diretórios no formato `nome-versão` e um nome simbólico `nome` que está anexado à versão recentemente instalada.

`/opt/aws/{apitools|amitools}/name/environment.sh`

Usado pelo `/etc/profile.d/aws-apitools-common.sh` para definir variáveis do ambiente específicas do produto, como `EC2_HOME`.

## Repositório de pacotes

O Amazon Linux 2 e o Amazon Linux AMI foram criados para serem usados com repositórios de pacotes online hospedados em cada região da AWS para o Amazon EC2. Esses repositórios fornecem atualizações contínuas para pacotes no Amazon Linux 2 e no Amazon Linux AMI, assim como acesso a centenas de aplicações adicionais de servidores de código aberto comuns. Os repositórios estão disponíveis em todas as regiões e são acessados com ferramentas de atualização `yum`. Hospedar repositórios em cada região nos permite implantar as atualizações rapidamente e sem nenhum encargo de transferência de dados.

O Amazon Linux 2 e o Amazon Linux AMI são atualizados regularmente com aprimoramentos de segurança e recursos. Se você não precisa preservar dados nem personalizações para suas instâncias, basta iniciar novamente as novas instâncias com a AMI atual. Se precisar preservar dados ou personalizações para suas instâncias, mantenha essas instâncias por meio dos repositórios de pacotes do Amazon Linux. Esses repositórios contêm todos os pacotes atualizados. Você pode escolher aplicar essas atualizações às suas instâncias em execução. As versões mais antigas dos pacotes de atualizações e AMIs continuarão disponíveis para uso, mesmo quando novas versões forem lançadas.

### Important

Sua instância deve ter acesso à Internet para acessar o repositório.

Para instalar pacotes, use o comando a seguir:

```
[ec2-user ~]$ sudo yum install package
```

Na Amazon Linux AMI, o acesso ao repositório Extra Packages for Enterprise Linux (EPEL) está configurado, mas não vem habilitado por padrão. O Amazon Linux 2 não está configurado para usar o repositório EPEL. O EPEL fornece pacotes de terceiros além dos que estão nos repositórios. A não

oferece suporte a pacotes de terceiro AWS. Você pode habilitar o repositório EPEL com os comandos a seguir:

- Para Amazon Linux 2:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- Para o Amazon Linux AMI:

```
[ec2-user ~]$ sudo yum-config-manager --enable epel
```

Se você descobrir que o Amazon Linux não contém uma aplicação de que precisa, pode simplesmente instalar essa aplicação diretamente em sua instância do Amazon Linux. O Amazon Linux usa RPMs e yum para gerenciamento de pacotes, e provavelmente essa é a maneira mais simples de instalar novas aplicações. Você sempre deve verificar se uma aplicação está disponível em nosso repositório central do Amazon Linux primeiro, porque muitas aplicações estão disponíveis nele. Essas aplicações podem ser facilmente adicionadas à sua instância Amazon Linux.

Para fazer upload de suas aplicações em uma instância do Amazon Linux em execução, use scp ou sftp e configure a aplicação fazendo login em sua instância. As aplicações também podem ser carregadas durante a execução da instância usando a ação PACKAGE\_SETUP no pacote cloud-init incorporado. Para obter mais informações, consulte [cloud-init \(p. 179\)](#).

## Atualizações de segurança

As atualizações de segurança são fornecidas pelos repositórios de pacotes, bem como por meio dos alertas de segurança de AMIs atualizados publicados no [Centro de segurança do Amazon Linux](#). Para obter mais informações sobre as políticas de segurança da AWS ou para informar um problema de segurança, acesse o [Centro de segurança da AWS](#).

O Amazon Linux é configurado para fazer download e instalar atualizações de segurança importantes ou essenciais no momento da execução. Recomendamos fazer as atualizações necessárias para seu caso de uso após a execução. Por exemplo: você pode aplicar todas as atualizações (não apenas as de segurança) na execução ou avaliar cada atualização e fazer apenas as aplicáveis ao seu sistema. Isso é controlado pela configuração cloud-init: `repo_upgrade`. O snippet da configuração cloud-init a seguir mostra como alterar as configurações no texto de dados do usuário que você transmite para a inicialização da instância:

```
#cloud-config
repo_upgrade: security
```

Os valores possíveis para `repo_upgrade` são os seguintes:

`critical`

Aplicar atualizações de segurança essenciais pendentes.

`important`

Aplicar atualizações de segurança importantes e essenciais pendentes.

`medium`

Aplicar atualizações de segurança pendentes essenciais, importantes e médias.

`low`

Aplicar todas as atualizações de segurança pendentes, incluindo atualizações de segurança de baixa gravidade.

**security**

Faça as atualizações essenciais ou importantes que a Amazon marca como atualizações de segurança.

**bugfix**

Aplicar atualizações que a Amazon marca como correções de erros. As correções de erros são um conjunto maior de atualizações, que incluem atualizações de segurança e correções para vários erros menores.

**all**

Aplicar todas as atualizações disponíveis aplicáveis, independentemente da classificação.

**none**

Não aplicar nenhuma atualização à instância no startup.

A configuração padrão para `repo_upgrade` é segurança. Ou seja, se você não especificar um valor diferente em seus dados do usuário, por padrão, o Amazon Linux executará as atualizações de segurança no lançamento para todos os pacotes instalados nesse momento. O Amazon Linux também o notifica sobre quaisquer atualizações nos pacotes instalados, listando o número de atualizações disponíveis após o login usando o arquivo `/etc/motd`. Para instalar essas atualizações, você precisa executar o comando `sudo yum upgrade` na instância.

## Configuração de repositórios

Com o Amazon Linux, as AMIs são tratadas como snapshots no tempo, com um repositório e uma estrutura de atualização que sempre fornece os pacotes mais recentes quando você executa `yum update -y`.

A estrutura do repositório é configurada para fornecer um fluxo contínuo de atualizações que permitem migrar de uma versão do Amazon Linux para a seguinte. Por exemplo, se você executar uma instância de uma versão mais antiga da AMI do Amazon Linux (como 2017.09 ou anterior) e executar `yum update -y`, você terminará com os pacotes mais recentes.

Você pode desabilitar as atualizações acumuladas habilitando o recurso bloquear na execução. O recurso de bloqueio na execução bloqueia sua instância para receber atualizações somente da versão especificada da AMI. Por exemplo, você pode executar uma AMI 2017.09 definir que ela receba somente as atualizações que forem liberadas antes da AMI 2018.03, até que você esteja pronto para migrar para a AMI 2018.03.

**Important**

Se você bloquear para uma versão dos repositórios que não seja a mais recente, não receberá atualizações adicionais. Para receber um fluxo contínuo de atualizações, você deve usar a AMI mais recente ou atualizar de forma consistente sua AMI com os repositórios apontados para a mais recente.

Para ativar o bloqueio na execução em novas instâncias, execute-a com os seguintes dados de usuário transmitidos para `cloud-init`:

```
#cloud-config
repo_releasever: 2017.09
```

Para bloquear as instâncias existentes em sua versão atual de AMI

1. Edite `/etc/yum.conf`.

2. Comente `releasever=latest`.
3. Para limpar o cache, execute `yum clean all`.

## Biblioteca de extras (Amazon Linux 2)

Com o Amazon Linux 2, você pode usar a Biblioteca de extras para instalar atualizações de aplicação e software em suas instâncias. Essas atualizações de software são conhecidas como tópicos. Você pode instalar uma versão específica de um tópico ou omitir informações de versão para usar a mais recente.

Para listar os tópicos disponíveis, use o comando a seguir:

```
[ec2-user ~]$ amazon-linux-extras list
```

Para ativar um tópico e instalar a versão mais recente do pacote a fim de garantir sua atualização, use o seguinte comando:

```
[ec2-user ~]$ sudo amazon-linux-extras install topic
```

Para ativar tópicos e instalar versões específicas de seus pacotes a fim de garantir a estabilidade, use o seguinte comando:

```
[ec2-user ~]$ sudo amazon-linux-extras install topic=version topic=version
```

Para remover um pacote instalado de um tópico, use o seguinte comando:

```
[ec2-user ~]$ sudo yum remove $(yum list installed | grep amzn2extra-topic | awk '{ print $1 }')
```

### Note

Esse comando não remove pacotes que foram instalados como dependências do adicional.

Para desabilitar um tópico e tornar os pacotes inacessíveis para o gerenciador de pacotes yum, use o seguinte comando:

```
[ec2-user ~]$ sudo amazon-linux-extras disable topic
```

### Important

Esse comando destina-se a usuários avançados. O uso inadequado desse comando pode causar conflitos de compatibilidade de pacotes.

## Acessar pacotes de origem para referência

Você pode visualizar a origem dos pacotes que você instalou em sua instância para fins de referência usando as ferramentas fornecidas no Amazon Linux. Os pacotes de origem estão disponíveis para todos os pacotes incluídos no Amazon Linux e no repositório de pacotes online. Basta determinar o nome do pacote de origem que você quer instalar e usar o comando `yumdownloader --source` para visualizar a origem em sua instância em execução. Por exemplo:

```
[ec2-user ~]$ yumdownloader --source bash
```

O RPM de origem pode ser desempacotado e, para referência, você poderá visualizar a árvore de origem usando ferramentas RPM padrão. Depois de encerrar a depuração, o pacote estará disponível para uso.

## cloud-init

O pacote cloud-init é uma aplicação de código aberto criado pela Canonical que é usado para inicializar imagens Linux em um ambiente de computação em nuvem, como o Amazon EC2. O Amazon Linux contém uma versão personalizada do cloud-init. Ele permite especificar as ações que devem acontecer em sua instância no momento da inicialização. Você pode transmitir ações desejadas para cloud-init por meio dos campos de dados do usuário ao executar uma instância. Isso significa que você pode usar AMIs comuns para muitos casos de uso e configurá-las dinamicamente no startup. O Amazon Linux também usa cloud-init para executar a configuração inicial da conta ec2-user.

Para obter mais informações, consulte a [documentação de cloud-init](#).

O Amazon Linux usa as ações de cloud-init localizadas em `/etc/cloud/cloud.cfg.d` e em `/etc/cloud/cloud.cfg`. Você pode criar seus próprios arquivos de ações de cloud-init em `/etc/cloud/cloud.cfg.d`. Todos os arquivos nesse diretório são lidos por cloud-init. Eles são lidos em ordem léxica e arquivos mais recentes substituem arquivos mais antigos.

O pacote cloud-init executa essas e outras tarefas de configuração comuns para as instâncias na inicialização:

- Definir o local padrão.
- Definir o nome do host.
- Analisar e lidar com os dados do usuário.
- Gerenciar chaves SSH privadas de host.
- Adicionar as chaves SSH públicas de um usuário ao `.ssh/authorized_keys` para facilitar login e administração.
- Preparar os repositórios para gerenciamento de pacotes.
- Lidar com as ações de pacotes definidas nos dados do usuário.
- Executar scripts de usuário encontrados nos dados do usuário.
- Montar volumes de armazenamento de instâncias, se aplicável.
  - Por padrão, o volume de armazenamento de instância `ephemeral0` será montado em `/media/ephemeral0` se estiver presente e possuir um sistema de arquivos válido; caso contrário, ele não será montado.
  - Por padrão, todos os volumes de troca associados à instância são montados (somente para os tipos de instância `m1.small` e `c1.medium`).
  - Você pode substituir a montagem do volume de armazenamento de instância padrão com a seguinte diretriz de cloud-init:

```
#cloud-config
mounts:
- [ ephemeral0 ]
```

Para obter mais informações sobre o controle sobre montagens, consulte [Montagens](#) na documentação do cloud-init.

- Os volumes de armazenamento de instâncias que oferecem suporte a TRIM não são formatados quando uma instância é iniciada, portanto, você deve partioná-los e formatá-los para poder montá-los. Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 1510\)](#). Você pode usar o módulo `disk_setup` para particionar e formatar seus volumes de armazenamento de instâncias na inicialização. Para obter mais informações, consulte [Configuração de discos](#) na documentação do cloud-init.

## Formatos de dados do usuário com suporte

O pacote cloud-init oferece suporte ao tratamento de dados do usuário de uma variedade dos formatos:

- Gzip
  - Se os dados do usuário forem compactados com gzip, o cloud-init descompactará os dados e os tratará adequadamente.
- Multipart MIME
  - Usando um arquivo multipart MIME, você pode especificar mais do que um tipo de dados. Por exemplo, você pode especificar um script de dados do usuário e um tipo de configuração de nuvem. Cada parte do arquivo multipart poderá ser tratada pelo cloud-init se for um dos formatos com suporte.
- Decodificação de base64
  - Se os dados do usuário forem codificados por base64, o cloud-init determinará se pode compreender os dados decodificados como um dos tipos com suporte. Se ele entender os dados decodificados, ele decodificará os dados e os tratará adequadamente. Caso contrário, ele retornará os dados base64 intactos.
- Script de dados do usuário
  - Começa com `#!` ou `Content-Type: text/x-shellscript`.
  - O script é executado pelo `/etc/init.d/cloud-init-user-scripts` durante o primeiro ciclo de inicialização. Isso ocorre tardiamente no processo de inicialização (depois que as ações de configuração inicial são executadas).
- Arquivo de inclusão
  - Começa com `#include` ou `Content-Type: text/x-include-url`.
  - Esse conteúdo é um arquivo de inclusão. O arquivo contém uma lista de URLs, um por linha. Cada URL é lido, e seu conteúdo é transmitido pelo mesmo conjunto de regras. O conteúdo lido do URL pode ser compactado por gzip, multipart MIME ou texto simples.
- Dados de config de nuvem
  - Começa com `#cloud-config` ou `Content-Type: text/cloud-config`.
  - Esse conteúdo são dados de configuração de nuvem. Veja exemplos comentados dos formatos de configuração com suporte.
- Trabalho de inicialização (não compatível com o Amazon Linux 2)
  - Começa com `#upstart-job` ou `Content-Type: text/upstart-job`.
  - Este conteúdo é armazenado em um arquivo em `/etc/init`, e a inicialização consome o conteúdo de acordo com outros trabalhos de inicialização.
- Cloud Boothook
  - Começa com `#cloud-boothook` ou `Content-Type: text/cloud-boothook`.
  - Esse conteúdo são dados boothook. São armazenados em um arquivo em `/var/lib/cloud` e executados imediatamente.
  - Esse é o "gancho" mais antigo disponível. Não é fornecido nenhum mecanismo para executá-lo somente uma vez. O boothook deve cuidar disso por conta própria. Ele é fornecido com o ID de instância na variável de ambiente `INSTANCE_ID`. Use essa variável para fornecer um conjunto de uma vez por instância de dados boothook.

## Assinar notificações do Amazon Linux

Para ser notificado quando novas AMIs forem executadas, você pode se inscrever usando o Amazon SNS.

Para assinar as notificações do Amazon Linux

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, já que a notificação do SNS que está assinando foi criada nesta região.
3. No painel de navegação, escolha Assinaturas, Criar assinatura.
4. Na caixa de diálogo Create subscription, faça o seguinte:
  - a. [Amazon Linux 2] Para o ARN do tópico, copie e cole o seguinte ARN (nome de recurso da Amazon): **arn:aws:sns:us-east-1:137112412989:amazon-linux-2-ami-updates**.
  - b. [Amazon Linux] Para o ARN do tópico, copie e cole o seguinte ARN (nome de recurso da Amazon): **arn:aws:sns:us-east-1:137112412989:amazon-linux-ami-updates**.
  - c. Em Protocol (Protocolo), escolha Email.
  - d. Em Endpoint, insira um endereço de e-mail que possa ser usado para receber notificações.
  - e. Selecione Create subscription.
5. Você receberá um e-mail de confirmação com o assunto "Notificação da AWS – confirmação de assinatura". Abra o e-mail e escolha Confirm subscription para concluir a assinatura.

Sempre que AMIs são lançadas, enviamos notificações aos assinantes do tópico correspondente. Para deixar de receber essas notificações, use o procedimento a seguir e cancele a inscrição.

#### Para cancelar a assinatura de notificações do Amazon Linux

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 a região na qual a notificação do SNS foi criada.
3. No painel de navegação, escolha Subscriptions (Assinaturas), selecione a assinatura e escolha Actions (Ações), Delete subscriptions (Excluir assinaturas).
4. Quando a confirmação for solicitada, escolha Excluir.

#### Formato da mensagem da AMI do SNS para Amazon Linux

O esquema para a mensagem do SNS é o seguinte.

```
{  
    "description": "Validates output from AMI Release SNS message",  
    "type": "object",  
    "properties": {  
        "v1": {  
            "type": "object",  
            "properties": {  
                "ReleaseVersion": {  
                    "description": "Major release (ex. 2018.03)",  
                    "type": "string"  
                },  
                "ImageVersion": {  
                    "description": "Full release (ex. 2018.03.0.20180412)",  
                    "type": "string"  
                },  
                "ReleaseNotes": {  
                    "description": "Human-readable string with extra information",  
                    "type": "string"  
                },  
                "Regions": {  
                    "type": "object",  
                    "description": "Each key will be a region name (ex. us-east-1)",  
                    "additionalProperties": {  
                        "type": "array",  
                        "items": {  
                            "type": "string"  
                        }  
                    }  
                }  
            }  
        }  
    }  
}
```

```
        "type": "object",
        "properties": {
            "Name": {
                "description": "AMI Name (ex. amzn-ami-hvm-2018.03.0.20180412-x86_64-gp2)",
                "type": "string"
            },
            "ImageId": {
                "description": "AMI Name (ex. ami-467ca739)",
                "type": "string"
            }
        },
        "required": [
            "Name",
            "ImageId"
        ]
    }
},
"required": [
    "ReleaseVersion",
    "ImageVersion",
    "ReleaseNotes",
    "Regions"
]
}
,
"required": [
    "v1"
]
}
```

## Executar o Amazon Linux 2 como máquina virtual no local

Use as imagens de máquina virtual (VM) do Amazon Linux 2 para o desenvolvimento e teste locais. Essas imagens estão disponíveis para uso nas seguintes plataformas de virtualização:

- VMWare
- KVM
- VirtualBox (Oracle VM)
- Microsoft Hyper-V

Para usar as imagens de máquinas virtuais do Amazon Linux 2 com uma das plataformas de virtualização compatíveis, é necessário fazer o seguinte:

- Etapa 1: preparar a imagem de inicialização `seed.iso` (p. 182)
- Etapa 2: fazer download da imagem da VM do Amazon Linux 2 (p. 184)
- Etapa 3: inicializar e conectar-se à sua nova VM (p. 184)

### Etapa 1: preparar a imagem de inicialização `seed.iso`

A imagem de inicialização `seed.iso` inclui as informações de configuração inicial necessárias para inicializar sua nova VM, como a configuração de rede, o nome do host e os dados do usuário.

### Note

A imagem de inicialização `seed.iso` inclui somente as informações de configuração necessárias para inicializar a VM. Ela não inclui os arquivos do sistema operacional do Amazon Linux 2.

Para gerar a imagem de inicialização `seed.iso`, você precisa dois arquivos de configuração:

- `meta-data`—Esse arquivo inclui o nome do host e as configurações de rede estática da VM.
- `user-data`—Esse arquivo configura as contas de usuário e especifica senhas, pares de chaves e mecanismos de acesso. Por padrão, a imagem da VM do Amazon Linux 2 cria uma conta de usuário `ec2-user`. Você usa o arquivo de configuração `user-data` para definir a senha da conta de usuário padrão.

Para criar o disco de inicialização **`seed.iso`**

1. Crie uma nova pasta chamada `seedconfig` e navegue até ela.
2. Crie o arquivo de configuração `meta-data`.
  - a. Crie um novo arquivo chamado `meta-data`.
  - b. Abra o arquivo `meta-data` usando o editor de texto de sua preferência e adicione o seguinte:

```
local-hostname: vm_hostname
# eth0 is the default network interface enabled in the image. You can configure
static network settings with an entry like the following.
network-interfaces: |
    auto eth0
    iface eth0 inet static
        address 192.168.1.10
        network 192.168.1.0
        netmask 255.255.255.0
        broadcast 192.168.1.255
        gateway 192.168.1.254
```

Substitua `vm_hostname` pelo nome do host da VM de sua escolha e defina as configurações da rede conforme necessário.

- c. Salve e feche o arquivo de configuração `meta-data`.

Para ver um exemplo do arquivo de configuração `meta-data` que especifica o nome do host da VM (`amazonlinux.onprem`), configura a interface de rede padrão (`eth0`) e especifica endereços IP estáticos para os dispositivos de rede necessários, consulte o [arquivo Seed.iso de exemplo](#).

3. Crie o arquivo de configuração `user-data`.
  - a. Crie um novo arquivo chamado `user-data`.
  - b. Abra o arquivo `user-data` usando o editor de texto de sua preferência e adicione o seguinte:

```
#cloud-config
#vim:syntax=yaml
users:
  # A user by the name `ec2-user` is created in the image by default.
  - default
chpasswd:
  list: |
    ec2-user:plain_text_password
  # In the above line, do not add any spaces after 'ec2-user:'.
```

Substitua `plain_text_password` por uma senha de sua escolha para a conta de usuário `ec2-user` padrão.

- c. (Opcional) Por padrão, o cloud-init aplica as configurações de rede sempre que a VM é inicializada. Adicione o seguinte para evitar que o cloud-init aplique configurações de rede a cada inicialização e retenha as configurações de rede aplicadas durante a primeira inicialização.

```
# NOTE: Cloud-init applies network settings on every boot by default. To retain
network settings from first
boot, add following 'write_files' section:
write_files:
  - path: /etc/cloud/cloud.cfg.d/80_disable_network_after_firstboot.cfg
    content: |
      # Disable network configuration after first boot
      network:
        config: disabled
```

- d. Salve e feche o arquivo de configuração `user-data`.

Também é possível criar contas de usuário adicionais e especificar seus mecanismos de acesso, senhas e pares de chave. Para obter mais informações sobre as diretivas compatíveis, consulte [Módulos](#). Para ver um exemplo do arquivo `user-data` que cria três usuários adicionais e especifica uma senha personalizada para a conta de usuário `ec2-user` padrão, consulte o [arquivo Seed.iso de exemplo](#).

4. Crie a imagem de inicialização `seed.iso` usando os arquivos de configuração `meta-data` e `user-data`.

Para Linux, use uma ferramenta como `genisoimage`. Navegue até a pasta `seedconfig` e execute o comando a seguir.

```
$ genisoimage -output seed.iso -volid cidata -joliet -rock user-data meta-data
```

Para macOS, use uma ferramenta como `hdiutil`. Navegue para um nível acima da pasta `seedconfig` e execute o comando a seguir.

```
$ hdiutil makehybrid -o seed.iso -hfs -joliet -iso -default-volume-name cidata
seedconfig/
```

## Etapa 2: fazer download da imagem da VM do Amazon Linux 2

Oferecemos uma imagem de VM do Amazon Linux 2 diferente para cada uma das plataformas de virtualização compatíveis. Faça download da imagem da VM correta para sua plataforma escolhida:

- [VMWare](#)
- [KVM](#)
- [Oracle VirtualBox](#)
- [Microsoft Hyper-V](#)

## Etapa 3: inicializar e conectar-se à sua nova VM

Para inicializar e conectar-se à sua nova VM, você deve ter a imagem de inicialização `seed.iso` (criada na Etapa 1) e uma imagem da VM do Amazon Linux 2 (obtida por download na Etapa 2). As etapas variam dependendo da plataforma da VM escolhida.

## VMWare vSphere

A imagem da VM para o VMware é disponibilizada no formato OVF.

### Como inicializar a VM usando o VMWare vSphere

1. Crie um datastore para o arquivo `seed.iso` ou adicione-o a um datastore existente.
2. Implante o modelo OVF, mas ainda não inicie a VM.
3. No painel Navegador, clique com o botão direito do mouse na nova máquina virtual e selecione Editar configurações.
4. Na guia Hardware virtual, em Novo dispositivo, selecione Unidade de CD/DVD e Adicionar.
5. Em Nova unidade de CD/DVD, selecione Arquivo ISO do datastore. Selecione o datastore ao qual você adicionou o arquivo `seed.iso`, procure e selecione o arquivo `seed.iso` e selecione OK.
6. Em Nova unidade de CD/DVD, selecione Conectar e OK.

Depois de associar o datastore à VM, você deverá ser capaz de inicializá-la.

## KVM

### Como inicializar a VM usando o KVM

1. Abra o assistente Criar VM.
2. Na Etapa 1, selecione Importar imagem de disco existente.
3. Na Etapa 2, procure e selecione a imagem da VM. Para Tipo de SO e Versão, selecione Linux e Red Hat Enterprise Linux 7.0, respectivamente.
4. Na Etapa 3, especifique a quantidade de RAM e o número de CPUs a serem usadas.
5. Na Etapa 4, insira um nome para a nova VM, selecione Personalizar configuração antes da instalação e Concluir.
6. Na janela Configuração da VM, selecione Adicionar hardware.
7. Na janela Adicionar novo hardware virtual, selecione Armazenamento.
8. Na Configuração de armazenamento, selecione Selecionar ou criar armazenamento personalizado. Em Tipo de dispositivo, selecione Dispositivo de CD-ROM. Selecione Gerenciar, Procurar local e procure e selecione o arquivo `seed.iso`. Escolha Finish.
9. Selecione Iniciar instalação.

## Oracle VirtualBox

### Como inicializar a VM usando o Oracle VirtualBox

1. Abra o Oracle VirtualBox e selecione New (Novo).
2. Em Name (Nome), insira um nome descritivo para a máquina virtual e, em Type (Tipo) e Version (Versão), selecione Linux e Red Hat (64 bits), respectivamente. Escolha Continue.
3. Em Memory size (Tamanho da memória), especifique a quantidade de memória a ser alocada para a máquina virtual e selecione Continue (Continuar).
4. Em Hard disk (Disco rígido), selecione Use an existing virtual hard disk file (Usar um arquivo de disco rígido virtual existente), navegue até a imagem da VM, abra-a e selecione Create (Criar).
5. Antes de iniciar a VM, é necessário carregar o arquivo `seed.iso` na unidade óptica virtual da máquina virtual:
  - a. Escolha a nova VM, selecione Configurações e Armazenamento.

- b. Na lista Storage Devices (Dispositivos de armazenamento), em Controller: IDE (Controlador: IDE), selecione a unidade óptica Empty (Vazio).
- c. Na seção Atributos da unidade óptica, selecione o botão de pesquisa, depois, Escolher arquivo de disco óptico virtual e selecione o arquivo seed.iso. Selecione OK para aplicar as alterações e feche as configurações.

Depois de adicionar o arquivo seed.iso à unidade óptica virtual, você poderá iniciar a VM.

#### Microsoft Hyper-V

A imagem da VM do Microsoft Hyper-V está compactada em um arquivo zip. É necessário extrair o conteúdo do arquivo zip.

#### Como inicializar a VM usando o Microsoft Hyper-V

1. Abra o New Virtual Machine Wizard (Novo assistente de máquina virtual).
2. Quando solicitado a escolher uma geração, selecione Geração 1.
3. Quando solicitado a configurar o adaptador de rede, em Conexão, selecione Externo.
4. Quando solicitado a conectar um disco rígido virtual, selecione Usar um disco rígido virtual existente, Procurar e procure e selecione a imagem da VM. Selecione Concluir para criar a VM.
5. Clique com o botão direito do mouse na nova VM e selecione Configurações. Na janela Configurações, em Controlador IDE 1, selecione Unidade de DVD.
6. Para a unidade de DVD, selecione Arquivo de imagem, procure e selecione o arquivo seed.iso.
7. Aplique as alterações e inicie a VM.

Após a inicialização da VM, faça login usando uma das contas de usuário definidas no arquivo de configuração user-data. Depois de ter feito login pela primeira vez, você pode desconectar a imagem de inicialização seed.iso da VM.

## Kernel Live Patching no Amazon Linux 2

O Kernel Live Patching para Amazon Linux 2 permite que você aplique vulnerabilidades de segurança e patches de erros críticos a um kernel do Linux em execução, sem reinicializações ou interrupções a aplicações de execução. Isso permite que você se beneficie de uma melhor disponibilidade de serviços e aplicações, mantendo sua infraestrutura segura e atualizada.

A AWS disponibiliza dois tipos de patches ao vivo do kernel para Amazon Linux 2:

- Atualizações de segurança – incluem atualizações para vulnerabilidades e exposições comuns (CVEs) do Linux. Normalmente, essas atualizações são classificadas como importantes ou críticas de acordo com as classificações do Boletim de segurança do Amazon Linux. Geralmente, elas são mapeadas com uma pontuação 7 ou maior do Common Vulnerability Scoring System (CVSS – Sistema de pontuação de vulnerabilidades comuns). Em alguns casos, a AWS pode fornecer atualizações antes da atribuição de CVE. Nesses casos, os patches podem aparecer como correções de erros.
- Correções de erros – incluem correções de erros críticos e problemas de estabilidade que não estão associados às CVEs.

A AWS disponibiliza patches ao vivo do kernel para uma versão do kernel para Amazon Linux 2 por até 3 meses depois de seu lançamento. Após o período de 3 meses, você deve fazer a atualização para uma versão posterior do kernel para continuar a receber patches ao vivo do kernel.

Os patches ao vivo do kernel para Amazon Linux 2 são disponibilizados como pacotes RPM assinados nos repositórios existentes do Amazon Linux 2. Os patches podem ser instalados em instâncias individuais

usando fluxos de trabalho yum existentes ou podem ser instalados em um grupo de instâncias gerenciadas usando o AWS Systems Manager.

O Kernel Live Patching no Amazon Linux 2 é fornecido sem custo adicional.

#### Tópicos

- [Configurações e pré-requisitos compatíveis \(p. 187\)](#)
- [Trabalhar com o Kernel Live Patching \(p. 187\)](#)
- [Limitations \(p. 191\)](#)
- [Perguntas frequentes \(p. 191\)](#)

## Configurações e pré-requisitos compatíveis

O Kernel Live Patching é compatível em instâncias do Amazon EC2 e [máquinas virtuais locais \(p. 182\)](#) que executam Amazon Linux 2.

Para usar o Kernel Live Patching no Amazon Linux 2, use:

- Uma arquitetura de 64 bits (x86\_64) compatível com o Amazon Linux 2
- O Amazon Linux 2 com a versão 4.14.165-131.185 ou posterior do kernel

#### Note

A arquitetura ARM de 64 bits (arm64) não é compatível.

## Trabalhar com o Kernel Live Patching

Você pode habilitar e usar o Kernel Live Patching em instâncias individuais usando a linha de comando na própria instância ou pode habilitar e usar o Kernel Live Patching em um grupo de instâncias gerenciadas usando o AWS Systems Manager.

As seções a seguir explicam como habilitar e usar o Kernel Live Patching em instâncias individuais usando a linha de comando.

Para obter mais informações sobre como habilitar e usar o Kernel Live Patching em um grupo de instâncias gerenciadas, consulte [Usar o Kernel Live Patching em instâncias do Amazon Linux 2](#) no Guia do usuário do AWS Systems Manager.

#### Tópicos

- [Habilitar o Kernel Live Patching \(p. 187\)](#)
- [Visualizar os patches ao vivo do kernel disponíveis \(p. 189\)](#)
- [Aplicar patches ao vivo do kernel \(p. 189\)](#)
- [Visualizar os patches ao vivo do kernel aplicados \(p. 190\)](#)
- [Desabilitar o Kernel Live Patching \(p. 191\)](#)

## Habilitar o Kernel Live Patching

O Kernel Live Patching está desabilitado por padrão no Amazon Linux 2. Para usar a aplicação de patches ao vivo, é necessário instalar o plug-in yum para o Kernel Live Patching e habilitar a funcionalidade de aplicação de patches ao vivo.

#### Prerequisites

O Kernel Live Patching requer `binutils`. Se você não tiver `binutils` instalado, instale-o usando o seguinte comando:

```
$ sudo yum install binutils
```

### Como habilitar o Kernel Live Patching

1. Os patches ao vivo do kernel estão disponíveis para Amazon Linux 2 com a versão `4.14.165-131.185` ou posterior do kernel. Para verificar a versão do kernel, execute o comando a seguir.

```
$ sudo yum list kernel
```

2. Se você já tiver uma versão do kernel compatível, ignore esta etapa. Se você não tiver uma versão do kernel compatível, execute os comandos a seguir para atualizar o kernel para a versão mais recente e reinicializar a instância.

```
$ sudo yum install -y kernel
```

```
$ sudo reboot
```

3. Instale o plug-in yum para o Kernel Live Patching.

```
$ sudo yum install -y yum-plugin-kernel-livepatch
```

4. Habilite o plug-in yum para o Kernel Live Patching.

```
$ sudo yum kernel-livepatch enable -y
```

Este comando também instala a versão mais recente de RPM do patch ao vivo do kernel a partir dos repositórios configurados.

5. Para confirmar se o plug-in yum para a aplicação de patches ao vivo no kernel foi instalado com êxito, execute o comando a seguir.

```
$ rpm -qa | grep kernel-livepatch
```

Quando você habilita o Kernel Live Patching, um RPM de patch ao vivo do kernel vazio é aplicado automaticamente. Se o Kernel Live Patching tiver sido habilitado com êxito, este comando retornará uma lista que inclui o RPM do patch ao vivo do kernel vazio inicial.

6. Instale o pacote kpatch.

```
$ sudo yum install -y kpatch-runtime
```

7. Atualize o serviço kpatch, caso tenha sido instalado anteriormente.

```
$ sudo yum update kpatch-runtime
```

8. Inicie o serviço kpatch. Este serviço carrega todos os patches ao vivo do kernel durante ou após a inicialização.

```
$ sudo systemctl enable kpatch.service
```

9. Configure o repositório do Kernel Live Patching para Amazon Linux 2, que contém os patches ao vivo do kernel.

```
$ sudo amazon-linux-extras enable livepatch
```

## Visualizar os patches ao vivo do kernel disponíveis

Os alertas de segurança do Amazon Linux são publicados no Centro de segurança do Amazon Linux. Para obter mais informações sobre os alertas de segurança do Amazon Linux 2, que incluem alertas para patches ao vivo do kernel, consulte o [Centro de segurança do Amazon Linux](#). Os patches ao vivo do kernel são prefixados com ALASLIVEPATCH. O Centro de segurança do Amazon Linux pode não listar patches ao vivo do kernel que resolvam erros.

Você também pode descobrir os patches ao vivo do kernel disponíveis para recomendações e CVEs usando a linha de comando.

Como listar todos os patches ao vivo do kernel disponíveis para recomendações

Use o seguinte comando.

```
$ yum updateinfo list
```

Veja a seguir um exemplo de saída.

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-motd
ALAS2LIVEPATCH-2020-002 important/Sec. kernel-
livepatch-4.14.165-133.209-1.0-3.amzn2.x86_64
ALAS2LIVEPATCH-2020-005 medium/Sec. kernel-livepatch-4.14.165-133.209-1.0-4.amzn2.x86_64
updateinfo list done
```

Como listar todos os patches ao vivo do kernel disponíveis para CVEs

Use o seguinte comando.

```
$ yum updateinfo list cves
```

Veja a seguir um exemplo de saída.

```
Loaded plugins: extras_suggestions, kernel-livepatch, langpacks, priorities, update-
motd
motd
amzn2-core/2/x86_64 | 2.4 kB 00:00:00
CVE-2019-15918 important/Sec. kernel-livepatch-4.14.165-133.209-1.0-3.amzn2.x86_64
CVE-2019-20096 important/Sec. kernel-livepatch-4.14.165-133.209-1.0-3.amzn2.x86_64
CVE-2020-8648 medium/Sec. kernel-livepatch-4.14.165-133.209-1.0-4.amzn2.x86_64
updateinfo list done
```

## Aplicar patches ao vivo do kernel

Aplique patches ao vivo do kernel usando o gerenciador de pacotes yum da mesma maneira que você aplicaria atualizações regulares. O plug-in yum para o Kernel Live Patching gerencia os patches ao vivo do kernel que devem ser aplicados e elimina a necessidade de reinicialização.

Tip

Recomendamos que você atualize seu kernel regularmente usando o Kernel Live Patching para garantir que ele continue seguro e atualizado.

Você pode optar por aplicar um patch ao vivo do kernel específico, ou aplicar qualquer patch ao vivo do kernel disponível com suas atualizações de segurança regulares.

## Como aplicar um patch ao vivo do kernel específico

1. Obtenha a versão do patch ao vivo do kernel usando um dos comandos descritos em [Visualizar os patches ao vivo do kernel disponíveis \(p. 189\)](#).
2. Aplique o patch ao vivo do kernel no kernel do Amazon Linux 2.

```
$ sudo yum install kernel-livepatch-kernel_version.x86_64
```

Por exemplo, o comando a seguir aplica um patch ao vivo do kernel para a versão Amazon Linux 2 do kernel 4.14.165-133.209.

```
$ sudo yum install kernel-livepatch-4.14.165-133.209-1.0-4.amzn2.x86_64
```

## Como aplicar patches ao vivo do kernel disponíveis com as atualizações de segurança regulares

Use o seguinte comando.

```
$ sudo yum update --security
```

Omita a opção `--security` para incluir correções de erros.

### Important

- A versão do kernel não é atualizada após a aplicação de patches ao vivo do kernel. A versão só é atualizada para a nova versão depois da reinicialização da instância.
- Um kernel do Amazon Linux 2 recebe patches ao vivo do kernel por um período de três meses. Após o término desse período de três meses, nenhum novo patch ao vivo do kernel será lançado para essa versão do kernel. Para continuar a receber patches ao vivo do kernel após o período de três meses, você deve reiniciar a instância de modo a migrar para a nova versão do kernel, que continuará recebendo patches ao vivo do kernel pelos próximos três meses. Para verificar a janela de suporte para a versão do kernel, execute `yum kernel-livepatch supported`.

## Visualizar os patches ao vivo do kernel aplicados

### Como visualizar os patches ao vivo do kernel aplicados

Use o seguinte comando.

```
$ kpatch list
```

O comando retornará uma lista dos patches ao vivo do kernel de atualização de segurança carregados e instalados. A seguir está um exemplo de saída.

```
Loaded patch modules:  
livepatch_cifs_lease_buffer_len [enabled]  
livepatch_CVE_2019_20096 [enabled]  
livepatch_CVE_2020_8648 [enabled]  
  
Installed patch modules:  
livepatch_cifs_lease_buffer_len (4.14.165-133.209.amzn2.x86_64)  
livepatch_CVE_2019_20096 (4.14.165-133.209.amzn2.x86_64)  
livepatch_CVE_2020_8648 (4.14.165-133.209.amzn2.x86_64)
```

### Note

Um único patch ao vivo do kernel pode incluir e instalar vários patches ao vivo.

## Desabilitar o Kernel Live Patching

Se não precisar mais usar o Kernel Live Patching, você pode desabilitá-lo a qualquer momento.

### Como desabilitar o Kernel Live Patching

1. Remova os pacotes RPM para os patches ao vivo do kernel aplicados.

```
$ sudo yum kernel-livepatch disable
```

2. Desinstale o plug-in yum para o Kernel Live Patching.

```
$ sudo yum remove yum-plugin-kernel-livepatch
```

3. Reinicialize a instância.

```
$ sudo reboot
```

## Limitations

O Kernel Live Patching tem as seguintes limitações:

- Ao aplicar um patch ao vivo no kernel, você não pode executar a hibernação, usar ferramentas avançadas de depuração (como SystemTap, kprobes e ferramentas baseadas em eBPF) ou acessar arquivos de saída ftrace usados pela infraestrutura do Kernel Live Patching.
- As instâncias do Amazon Linux 2 com arquitetura ARM de 64 bits (arm64) não são compatíveis.

## Perguntas frequentes

Para ver as perguntas frequentes sobre o Kernel Live Patching para Amazon Linux 2, consulte as [Perguntas frequentes sobre o Kernel Live Patching para Amazon Linux 2](#).

## Kernel fornecido pelo usuário

Se você precisar de um kernel personalizado nas instâncias do Amazon EC2, poderá iniciar com uma AMI próxima da que você deseja, compilar o kernel personalizado na instância e atualizar o bootloader para apontar para o novo kernel. Esse processo varia de acordo com o tipo de virtualização que sua AMI usa. Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#).

### Tópicos

- [AMIs HVM \(GRUB\) \(p. 191\)](#)
- [AMIs paravirtuais \(PV-GRUB\) \(p. 192\)](#)

## AMIs HVM (GRUB)

Volumes de instância HVM são tratados como discos físicos reais. O processo de inicialização é semelhante ao de um sistema operacional bare metal, com um disco particionado e um bootloader, que

permite a ele funcionar com todas as distribuições do Linux atualmente compatíveis. O bootloader mais comum é o GRUB ou o GRUB2.

Por padrão, o GRUB não envia sua saída para o console da instância, pois cria um atraso de inicialização a mais. Para obter mais informações, consulte [Saída do console da instância \(p. 1609\)](#). Se você estiver instalando um kernel personalizado, considere habilitar a saída do GRUB.

Não é necessário especificar um kernel de fallback, mas recomendamos que você tenha um fallback ao testar um novo kernel. O GRUB podem recuar para outro kernel no caso de o novo kernel falhar. Ter um kernel de fallback reserva permite que a instância seja inicializada mesmo se o novo kernel não for encontrado.

O GRUB herdado para o Amazon Linux usa `/boot/grub/menu.lst`. O GRUB2 para o Amazon Linux 2 usa `/etc/default/grub`. Para obter mais informações sobre como atualizar o kernel padrão no bootloader, consulte a documentação de sua distribuição do Linux.

## AMIs paravirtuais (PV-GRUB)

As Imagens de máquina da Amazon que usam virtualização paravirtual (PV) utilizam um sistema chamado PV-GRUB durante o processo de inicialização. PV-GRUB é um bootloader paravirtual que executa uma versão corrigida do GNU GRUB 0.97. Quando você inicia uma instância, o PV-GRUB inicia o processo de inicialização da cadeia e, em seguida, carrega o kernel especificado pelo arquivo da sua imagem `menu.lst`.

O PV-GRUB entende os comandos `grub.conf` ou `menu.lst` padrão, que permite que ele trabalhe com todas as distribuições do Linux atualmente suportadas. Distribuições mais antigas, como Ubuntu 10.04 LTS, Oracle Enterprise Linux ou CentOS 5.x, exigem um pacote especial de kernels "ec2" ou "xen", enquanto distribuições mais novas incluem os drivers necessários no pacote de kernel padrão.

A maioria das AMIs paravirtuais modernas usa uma AKI PV-GRUB padrão (incluindo todas as AMIs em Linux paravirtuais disponíveis no menu Início rápido do Launch Wizard do Amazon EC2), por isso não há etapas adicionais que você precisa tomar para usar um kernel diferente na sua instância, desde que o kernel desejado seja compatível com sua distribuição. A melhor maneira de executar um kernel personalizado na instância é começar com a AMI mais próxima à que você deseja, compilar o kernel personalizado na instância e modificar o arquivo `menu.lst` para ser inicializado com esse kernel.

É possível verificar se a imagem do kernel de uma AMI é uma AKI PV-GRUB. Execute o comando a seguir [describe-images](#) (substituindo seu ID de imagem do kernel) e verifique se o campo `Name` começa com `pv-grub`:

```
aws ec2 describe-images --filters Name=image-id,Values=aki-880531cd
```

### Tópicos

- [Limitações do PV-GRUB \(p. 192\)](#)
- [Configurar GRUB para AMIs paravirtuais \(p. 193\)](#)
- [IDs da imagem do kernel do PV-GRUB da Amazon \(p. 194\)](#)
- [Atualizar PV-GRUB \(p. 196\)](#)

## Limitações do PV-GRUB

O PV-GRUB tem as seguintes limitações:

- Você não pode usar a versão de 64 bits do PV-GRUB para iniciar um kernel de 32 bits ou vice-versa.

- Você não pode especificar uma imagem de ramdisk da Amazon (ARI) ao usar uma PV-GRUB AKI.
- AWSA testou e verificou que o PV-GRUB funciona com os seguintes formatos de sistema de arquivos: EXT2, EXT3, EXT4, JFS, XFS e ReiserFS. Outros formatos de sistema de arquivos podem não funcionar.
- O PV-GRUB pode inicializar os kernels compactados usando os formatos de compressão gzip, bzip2, lz e xz.
- As AMIs do cluster não oferecem suporte nem precisam de PV-GRUB, pois usam a virtualização completa do hardware (HVM). Enquanto instâncias paravirtuais usam PV-GRUB para iniciar, os volumes de instância de HVM são tratados como discos reais, e o processo de inicialização é semelhante ao processo de inicialização do sistema operacional bare metal com um disco particionado e um bootloader.
- O PV-GRUB versões 1.03 e anteriores não são compatíveis com particionamento de GPT; elas oferecem suporte somente a particionamento MBR.
- Se você planeja usar um gerenciador de volumes lógicos (LVM) com os volumes do Amazon Elastic Block Store (Amazon EBS), precisa de uma partição de inicialização separada do LVM. Então, você pode criar volumes lógicos com o LVM.

## Configurar GRUB para AMIs paravirtuais

Para inicializar PV-GRUB, deve existir um arquivo `menu.lst` do GRUB na imagem; a localização mais comum para esse arquivo é `/boot/grub/menu.lst`.

A seguir está um exemplo de um arquivo de configuração de `menu.lst` para inicializar uma AMI com uma PV-GRUB AKI. Neste exemplo, há duas entradas de kernel para escolher: do Amazon Linux 2018.03 (o kernel original desta AMI) e Vanilla Linux 4.16.4 (uma versão mais recente do kernel Vanilla Linux de <https://www.kernel.org/>). A entrada de Vanilla foi copiada da entrada original para essa AMI, e os caminhos `kernel` e `initrd` foram atualizados para os novos locais. O parâmetro `default 0` aponta o bootloader para a primeira entrada que vê (nesse caso, a entrada do Vanilla), e o parâmetro `fallback 1` aponta o bootloader para a entrada seguinte se houver um problema em inicializar o primeiro.

```
default 0
fallback 1
timeout 0
hiddenmenu

title Vanilla Linux 4.16.4
root (hd0)
kernel /boot/vmlinuz-4.16.4 root=LABEL=/ console=hvc0
initrd /boot/initrd.img-4.16.4

title Amazon Linux 2018.03 (4.14.26-46.32.amzn1.x86_64)
root (hd0)
kernel /boot/vmlinuz-4.14.26-46.32.amzn1.x86_64 root=LABEL=/ console=hvc0
initrd /boot/initramfs-4.14.26-46.32.amzn1.x86_64.img
```

Você não precisa especificar o kernel de fallback no seu arquivo `menu.lst`, mas recomendamos que você tenha um fallback ao testar um novo kernel. O PV-GRUB podem recuar para outro kernel no caso de o novo kernel falhar. Ter um kernel de fallback reserva permite que a instância initialize mesmo se o novo kernel não for encontrado.

O PV-GRUB verifica os seguintes locais quanto a `menu.lst` usando o primeiro que encontrar:

- `(hd0)/boot/grub`
- `(hd0,0)/boot/grub`
- `(hd0,0)/grub`
- `(hd0,1)/boot/grub`

- (hd0,1)/grub
- (hd0,2)/boot/grub
- (hd0,2)/grub
- (hd0,3)/boot/grub
- (hd0,3)/grub

Observe que PV-GRUB 1.03 e anteriores só verificam um dos dois primeiros locais dessa lista.

## IDs da imagem do kernel do PV-GRUB da Amazon

As AKIs do PV-GRUB estão disponíveis em todas as regiões do Amazon EC2, exceto a Ásia-Pacífico (Osaka). Há AKIs para os tipos de arquitetura de 32 e 64 bits. A maioria das AMIs modernas usa uma AKI PV-GRUB por padrão.

Recomendamos que você sempre use a versão mais recente da AKI PV-GRUB, pois nem todas as versões são compatíveis com todos os tipos de instância. Use o comando [describe-images](#) para obter uma lista de AKIs PV-GRUB para a região atual:

```
aws ec2 describe-images --owners amazon --filters Name=name,Values=pv-grub-* .gz
```

A PV-GRUB é a única AKI disponível na região ap-southeast-2. Você deve verificar se alguma AMI que deseja copiar para essa região está usando uma versão de PV-GRUB disponível nessa região.

Veja a seguir os IDs da AKI atuais de cada região. Registre novas AMIs usando uma AKI hd0.

### Note

Nós continuamos a fornecer AKIs hd00 para retrocompatibilidade nas regiões em que elas estavam disponíveis anteriormente.

ap-northeast-1, Asia Pacific (Tokyo)

ID da imagem	Nome da imagem
aki-f975a998	pv-grub-hd0_1.05-i386.gz
aki-7077ab11	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-1, Asia Pacific (Singapore) Region

ID da imagem	Nome da imagem
aki-17a40074	pv-grub-hd0_1.05-i386.gz
aki-73a50110	pv-grub-hd0_1.05-x86_64.gz

ap-southeast-2, Asia Pacific (Sydney)

ID da imagem	Nome da imagem
aki-ba5665d9	pv-grub-hd0_1.05-i386.gz
aki-66506305	pv-grub-hd0_1.05-x86_64.gz

eu-central-1, Europe (Frankfurt)

ID da imagem	Nome da imagem
aki-1419e57b	<code>pv-grub-hd0_1.05-i386.gz</code>
aki-931fe3fc	<code>pv-grub-hd0_1.05-x86_64.gz</code>

eu-west-1, Europe (Ireland)

ID da imagem	Nome da imagem
aki-1c9fd86f	<code>pv-grub-hd0_1.05-i386.gz</code>
aki-dc9ed9af	<code>pv-grub-hd0_1.05-x86_64.gz</code>

sa-east-1, South America (São Paulo)

ID da imagem	Nome da imagem
aki-7cd34110	<code>pv-grub-hd0_1.05-i386.gz</code>
aki-912fbcf9	<code>pv-grub-hd0_1.05-x86_64.gz</code>

us-east-1, US East (N. Virginia)

ID da imagem	Nome da imagem
aki-04206613	<code>pv-grub-hd0_1.05-i386.gz</code>
aki-5c21674b	<code>pv-grub-hd0_1.05-x86_64.gz</code>

us-gov-west-1, AWS GovCloud (US-West)

ID da imagem	Nome da imagem
aki-5ee9573f	<code>pv-grub-hd0_1.05-i386.gz</code>
aki-9ee55bff	<code>pv-grub-hd0_1.05-x86_64.gz</code>

us-west-1, US West (N. California)

ID da imagem	Nome da imagem
aki-43cf8123	<code>pv-grub-hd0_1.05-i386.gz</code>
aki-59cc8239	<code>pv-grub-hd0_1.05-x86_64.gz</code>

us-west-2, US West (Oregon)

ID da imagem	Nome da imagem
aki-7a69931a	<code>pv-grub-hd0_1.05-i386.gz</code>

ID da imagem	Nome da imagem
aki-70cb0e10	pv-grub-hd0_1.05-x86_64.gz

## Atualizar PV-GRUB

Recomendamos que você sempre use a versão mais recente da AKI PV-GRUB, pois nem todas as versões são compatíveis com todos os tipos de instância. Além disso, versões mais antigas do PV-GRUB não estão disponíveis em todas as regiões. Por isso, se você copiar uma AMI usando uma versão mais antiga para uma região que não oferece suporte a essa versão, será incapaz de inicializar as instâncias executadas a partir daquela AMI até que atualize a imagem do kernel. Use os procedimentos a seguir para verificar a versão da sua instância do PV-GRUB e atualizá-la, se necessário.

Para verificar sua versão do PV-GRUB

1. Encontre o ID do kernel para sua instância.

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute kernel --region region

{
    "InstanceId": "instance_id",
    "KernelId": "aki-70cb0e10"
}
```

O ID do kernel para essa instância é aki-70cb0e10.

2. Veja as informações de versão do ID desse kernel.

```
aws ec2 describe-images --image-ids aki-70cb0e10 --region region

{
    "Images": [
        {
            "VirtualizationType": "paravirtual",
            "Name": "pv-grub-hd0_1.05-x86_64.gz",
            ...
            "Description": "PV-GRUB release 1.05, 64-bit"
        }
    ]
}
```

Esta imagem do kernel é PV-GRUB 1.05. Se a versão do PV-GRUB não for a mais nova (conforme exibido em [IDs da imagem do kernel do PV-GRUB da Amazon \(p. 194\)](#)), atualize-a usando o procedimento a seguir.

Para atualizar sua versão do PV-GRUB

Se sua instância estiver usando uma versão mais antiga de PV-GRUB, atualize-a para a versão mais recente.

1. Identifique a AKI PV-GRUB mais recente para sua região e arquitetura de processadores de [IDs da imagem do kernel do PV-GRUB da Amazon \(p. 194\)](#).
2. Pare a instância. Sua instância deve ser interrompida para modificar a imagem do kernel usada.

```
aws ec2 stop-instances --instance-ids instance_id --region region
```

3. Modifique a imagem do kernel usada para sua instância.

```
aws ec2 modify-instance-attribute --instance-id instance_id --kernel kernel_id --region region
```

4. Reinicie sua instância.

```
aws ec2 start-instances --instance-ids instance_id --region region
```

## Configure a conexão de desktop MATE Amazon Linux 2

O ambiente de desktop MATE vem pré-instalado e pré-configurado na AMI com a seguinte descrição: Amazon Linux 2 com .Net Core, Mono e MATE Desktop Environment. O ambiente fornece uma interface gráfica de usuário intuitiva para administrar as instâncias Amazon Linux 2 sem usar a linha de comando. A interface usa representações gráficas, como ícones, janelas, barras de ferramentas, pastas, papéis de parede e widgets de desktop. Ferramentas integradas baseadas em GUI estão disponíveis para executar tarefas comuns. Por exemplo, existem ferramentas para adicionar e remover software, aplicar atualizações, organizar arquivos, iniciar programas e monitorar a integridade do sistema.

### Important

O xrdp é o software de Desktop Remoto incluído na AMI. Por padrão, o xrdp usa um certificado TLS autoassinado para criptografar sessões de desktop remoto. Nem a AWS nem os mantenedores do xrdp recomendam o uso de certificados autoassinados na produção. Em vez disso, obtenha um certificado de uma autoridade de certificação (CA) apropriada e instale-o em suas instâncias. Para obter mais informações sobre a configuração de TLS, consulte [TLS security layer](#) (Camada de segurança do TLS) na wiki do xrdp.

## Prerequisite

Para executar os comandos mostrados neste tópico, você deve instalar o AWS Command Line Interface (AWS CLI) ou AWS Tools for Windows PowerShell, e configurar o seu AWS perfil.

### Options

1. Instale a AWS CLI: para obter mais informações, consulte [Installing the AWS CLI](#) (Instalar a AWS CLI) e [Configuration basics](#) (Noções básicas de configuração) no Guia do usuário da AWS Command Line Interface.
2. Instale o Tools for Windows PowerShell: para obter mais informações, consulte [Installing the AWS Tools for Windows PowerShell](#) (Instalar o AWS Tools for Windows PowerShell) e [Shared credentials](#) (Credenciais compartilhadas) no AWS Tools for Windows PowerShell User Guide (Manual do usuário do AWS Tools for Windows PowerShell).

## Configure a conexão RDP

Siga estas etapas para configurar uma conexão RDP (Remote Desktop Protocol) a partir de sua máquina local para uma instância Amazon Linux 2 que estiver executando o ambiente de desktop MATE.

1. Para obter o ID da AMI para Amazon Linux 2, que inclui MATE no nome da AMI, use o comando [describe-imagens](#) da ferramenta da linha de comando local.

```
aws ec2 describe-images --filters "Name=name,Values=amzn2*MATE*" --query "Images[*].  
[ImageId,Name,Description]"  
[  
  [  
    "ami-0123example0abc12",  
    "amzn2-x86_64-MATEDE_DOTNET-2020.12.04",  
    ".NET Core 5.0, Mono 6.12, PowerShell 7.1, and MATE DE pre-installed to run  
    your .NET applications on Amazon Linux 2 with Long Term Support (LTS)."  
  ],  
  [  
    "ami-0456example0def34",  
    "amzn2-x86_64-MATEDE_DOTNET-2020.04.14",  
    "Amazon Linux 2 with .Net Core, PowerShell, Mono, and MATE Desktop Environment"  
  ]  
]
```

Escolha a AMI apropriada para seu uso.

2. Execute uma instância do EC2 com a AMI localizada na etapa anterior. Configure o grupo de segurança para permitir o tráfego TCP de entrada para a porta 3389. Para obter mais informações sobre como configurar grupos de segurança, consulte [Grupos de segurança para a VPC](#). Essa configuração permite que você use um cliente RDP para se conectar à instância.
3. Conecte-se à instância usando [SSH](#). Execute o comando a seguir na instância do Linux para definir a senha do `ec2-user`.

```
[ec2-user ~]$ sudo passwd ec2-user
```

4. Instale o certificado e a chave.

Se você já tiver um certificado e uma chave, copie-os para o diretório `/etc/xrdp/` da seguinte forma:

- Certificado — `/etc/xrdp/cert.pem`
- Chave — `/etc/xrdp/key.pem`

Se você não tiver um certificado e uma chave, use o seguinte comando para gerá-los no diretório `/etc/xrdp/`.

```
$ sudo openssl req -x509 -sha384 -newkey rsa:3072 -nodes -keyout /etc/xrdp/key.pem -  
out /etc/xrdp/cert.pem -days 365
```

#### Note

Esse comando gera um certificado válido por 365 dias.

5. Abra um cliente RDP no computador a partir do qual você se conectará à instância (por exemplo, Conexão de Desktop Remoto em um computador com Microsoft Windows). Insira `ec2-user` como o nome de usuário e digite a senha definida na etapa anterior.

#### Como desabilitar o ambiente de desktop MATE na instância do Amazon EC2

É possível desativar o ambiente GUI a qualquer momento executando um dos seguintes comandos na instância do Linux.

```
[ec2-user ~]$ sudo systemctl disable xrdp
```

```
[ec2-user ~]$ sudo systemctl stop xrdp
```

Como habilitar o ambiente de desktop MATE na instância do Amazon EC2

Para ativar a GUI novamente, é possível executar um dos seguintes comandos em na instância do Linux.

```
[ec2-user ~]$ sudo systemctl enable xrdp
```

```
[ec2-user ~]$ sudo systemctl start xrdp
```

# 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. \(p. 5\)](#)
- [Tutorial: Comece a usar instâncias Linux do Amazon EC2 \(p. 9\)](#)
- [Ciclo de vida da instância \(p. 503\)](#)

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 \(p. 203\)](#).

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 \(p. 338\)](#).

P: Que tipo de volume raiz atende às minhas necessidades?

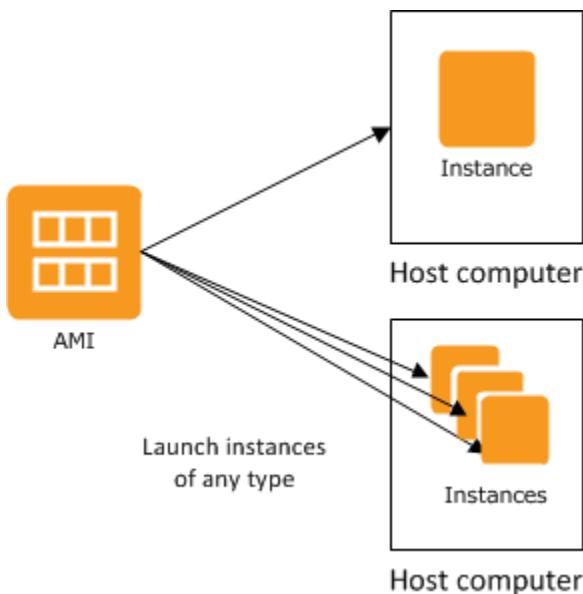
Cada instância é baseada no Amazon EBS ou no armazenamento de instâncias. Selecione uma AMI baseada no tipo de volume raiz necessário. Para obter mais informações, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#).

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 e AMIs

Uma Imagem de máquina da Amazon (AMI) é um modelo que contém uma configuração de software (por exemplo, sistema operacional, servidor de aplicação e aplicações). A partir de uma AMI, execute uma instância, que é uma cópia da AMI que roda como servidor virtual na nuvem. Você pode executar várias instâncias de uma AMI, conforme mostrado na figura a seguir.



Suas instâncias continuarão sendo executadas até que você as interrompa, hiberne ou encerre, ou até que elas falhem. Se uma instância falhar, você pode executar uma nova instância a partir da AMI.

## Instances

Uma instância é um servidor virtual na nuvem. A configuração na execução é uma cópia da AMI que você especificou ao executar a instância.

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 a aplicação ou 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).

Após executar a instância, ela se parecerá como um host tradicional e você poderá interagir com ela assim como com qualquer computador. Você tem controle total de suas instâncias. Você pode usar o sudo para executar os comandos que exigem privilégios raiz.

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 do Amazon EC2.

## Armazenamento para sua instância

O dispositivo raiz da sua instância contém a imagem usada para inicializar a instância. O dispositivo raiz é um volume do Amazon Elastic Block Store (Amazon EBS) ou um volume do armazenamento de instâncias. Para obter mais informações, consulte [Volume do dispositivo raiz da instância do Amazon EC2 \(p. 1521\)](#).

Sua instância pode incluir os volumes de armazenamento locais, conhecidos como volumes de armazenamento de instâncias, que você pode configurar o momento da execução com o mapeamento de dispositivos de blocos. Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1530\)](#). Depois de esses volumes serem adicionados e mapeados para sua instância, eles estarão disponíveis para você montar e usar. Se sua instância falhar, ou se sua instância for executada ou encerrada, os dados nesses volumes serão perdidos; portanto, esses volumes são mais bem usados

para dados temporários. Para manter a segurança de dados importantes, você deve usar uma estratégia de replicação em várias instâncias ou armazenar seus dados persistentes em volumes do Amazon S3 ou do Amazon EBS. Para obter mais informações, consulte [Storage \(p. 1247\)](#).

## Práticas recomendadas de segurança

- Use o AWS Identity and Access Management (IAM) para controlar o acesso aos seus recursos da AWS, incluindo suas instâncias. Você pode criar os usuários e grupos do IAM sob sua conta da AWS, atribuir credenciais de segurança a cada um e controlar o acesso que cada um tem aos recursos e produtos da AWS. Para obter mais informações, consulte [Identity and Access Management para o Amazon EC2 \(p. 1136\)](#).
- Restrinja o acesso permitindo somente que hosts ou redes confiáveis acessem as portas na sua instância. Por exemplo, você pode restringir o acesso a SSH ao restringir o tráfego de entrada na porta 22. Para obter mais informações, consulte [Grupos de segurança do Amazon EC2 para instâncias do Linux \(p. 1225\)](#).
- Revise as regras de seus grupos de segurança regularmente e aplique o princípio do menor privilégio: abra somente as permissões que forem necessárias. Você também pode criar security groups diferentes para lidar com instâncias com requisitos de segurança diferentes. Pense em criar um security group bastion que permita logins externos e mantenha o restante de suas instâncias em um grupo que não permita logins externos.
- Desabilite logins com senha das instâncias executadas a partir da sua AMI. As senhas podem ser localizadas ou roubadas, e são um risco para a segurança. Para obter mais informações, consulte [Desabilitar logins remotos com senha para raiz \(p. 99\)](#). Para obter mais informações sobre compartilhamento seguro das AMIs, consulte [AMIs compartilhadas \(p. 92\)](#).

## Interromper e encerrar instâncias

É possível interromper ou encerrar uma instância em execução a qualquer momento.

### Interromper uma instância

Quando uma instância for interrompida, ela executará a desativação normal e fará a transição para o estado stopped. Todos os volumes do Amazon EBS permanecem associados e você pode começar a instância novamente em um momento posterior.

Você não será cobrado pelo uso adicional da instância enquanto ela estiver em estado interrompido. Será cobrada uma de um minuto no mínimo para cada transição de um estado parado para um estado em execução. Se o tipo de instância tiver sido alterado quando a instância estava interrompida, será cobrada a taxa do novo tipo de instância depois de a instância ser iniciada. Qualquer uso da sua instância associado ao Amazon EBS , inclusive o uso do dispositivo raiz, será cobrado usando os preços regulares do Amazon EBS.

Quando uma instância estiver em um estado interrompido, você poderá associar ou separar os volumes do Amazon EBS. Você também pode criar AMIs a partir da instância e alterar o kernel, o disco de RAM e o tipo de instância.

### Como encerrar uma instância

Quando uma instância é encerrada, ela executa uma desligamento normal. O volume do dispositivo raiz é excluído por padrão, mas todos os volumes do Amazon EBS anexados são preservados por padrão, que é determinado pela configuração do atributo `deleteOnTermination` de cada volume. A instância em si também é excluída, e você não pode iniciá-la novamente em um momento posterior.

Para evitar encerramento acidental, você pode desabilitar o encerramento da instância. Se você fizer isso, garanta que o atributo `disableApiTermination` esteja definido como `true` para a instância. Para controlar o comportamento da desativação da instância, como `shutdown -h` em Linux ou `shutdown`

no Windows, defina o atributo da instância `instanceInitiatedShutdownBehavior` como `stop` ou `terminate`, conforme desejado. As instâncias com volumes do Amazon EBS para o dispositivo raiz usam `stop` como padrão, e as instâncias com dispositivos raiz de armazenamento de instâncias são sempre encerradas como resultado da desativação da instância.

Para obter mais informações, consulte [Ciclo de vida da instância \(p. 503\)](#).

#### Note

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 [Avoiding Unexpected Changes](#) (Evitar cobranças inesperadas) no AWS Billing and Cost Management User Guide (Guia do usuário do AWS Billing and Cost Management). Para obter mais informações sobre os custos do Amazon EBS, consulte a [Definição de preço do Amazon EBS](#).

## AMIs

A Amazon Web Services (AWS) publica muitas [imagens de máquina da Amazon \(AMIs\)](#) 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 pode 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 sua aplicação fica pronta para aceitar solicitações.

Todas as AMIs são classificadas como com Amazon EBS, o que significa que o dispositivo raiz da instância executada a partir da AMI é um volume do Amazon EBS ou com armazenamento de instâncias, o que significa que o dispositivo raiz da instância executada a partir da AMI é um volume de armazenamento de instâncias criado a partir de um modelo armazenado em Amazon S3.

A descrição de uma AMI indica o tipo de dispositivo raiz (`ebs` ou `instance store`). Isso é importante, pois há diferenças significativas quanto a que você pode fazer com cada tipo de AMI. Para obter mais informações sobre essas diferenças, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#).

Você pode cancelar o registro de uma AMI quando tiver terminado de usá-la. Depois de cancelar o registro de uma AMI, você não poderá usá-la para executar novas instâncias. As instâncias existentes executadas na AMI não são afetadas. Portanto, se você também tiver terminado com as instâncias executadas por essas AMIs, deverá encerrá-las.

## 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 \(p. 204\)](#)
- [Especificações de hardware \(p. 208\)](#)
- [Tipos de virtualização de AMI \(p. 209\)](#)
- [Instâncias criadas no Sistema Nitro \(p. 210\)](#)
- [Recursos de redes e armazenamento \(p. 211\)](#)
- [Limites de instâncias \(p. 214\)](#)
- [Instâncias de uso geral \(p. 214\)](#)
- [Instâncias otimizadas para computação \(p. 273\)](#)
- [Instâncias otimizadas para memória \(p. 282\)](#)
- [Instâncias otimizadas para armazenamento \(p. 297\)](#)
- [Linux Instâncias computacionais aceleradas do \(p. 305\)](#)
- [Localizar um tipo de instância do Amazon EC2 \(p. 326\)](#)
- [Alterar o tipo de instância \(p. 327\)](#)
- [Obter recomendações de um tipo de instância \(p. 334\)](#)

## 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 \(p. 326\)](#).

### 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. 273)
C5	c5.large   c5.xlarge   c5.2xlarge   c5.4xlarge   c5.9xlarge   c5.12xlarge   c5.18xlarge   c5.24xlarge   c5.metal	Otimizadas para computação (p. 273)
C5a	c5a.large   c5a.xlarge   c5a.2xlarge   c5a.4xlarge   c5a.8xlarge   c5a.12xlarge   c5a.16xlarge   c5a.24xlarge	Otimizadas para computação (p. 273)

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Tipos de instâncias disponíveis

Tipo	Sizes	Caso de uso
C5ad	c5ad.large   c5ad.xlarge   c5ad.2xlarge   c5ad.4xlarge   c5ad.8xlarge   c5ad.12xlarge   c5ad.16xlarge   c5ad.24xlarge	Otimizadas para computação ( <a href="#">p. 273</a> )
C5d	c5d.large   c5d.xlarge   c5d.2xlarge   c5d.4xlarge   c5d.9xlarge   c5d.12xlarge   c5d.18xlarge   c5d.24xlarge   c5d.metal	Otimizadas para computação ( <a href="#">p. 273</a> )
C5n	c5n.large   c5n.xlarge   c5n.2xlarge   c5n.4xlarge   c5n.9xlarge   c5n.18xlarge   c5n.metal	Otimizadas para computação ( <a href="#">p. 273</a> )
C6g	c6g.medium   c6g.large   c6g.xlarge   c6g.2xlarge   c6g.4xlarge   c6g.8xlarge   c6g.12xlarge   c6g.16xlarge   c6g.metal	Otimizadas para computação ( <a href="#">p. 273</a> )
C6gd	c6gd.medium   c6gd.large   c6gd.xlarge   c6gd.2xlarge   c6gd.4xlarge   c6gd.8xlarge   c6gd.12xlarge   c6gd.16xlarge   c6gd.metal	Otimizadas para computação ( <a href="#">p. 273</a> )
C6gn	c6gn.medium   c6gn.large   c6gn.xlarge   c6gn.2xlarge   c6gn.4xlarge   c6gn.8xlarge   c6gn.12xlarge   c6gn.16xlarge	Otimizadas para computação ( <a href="#">p. 273</a> )
D2	d2.xlarge   d2.2xlarge   d2.4xlarge   d2.8xlarge	Otimizada para armazenamento ( <a href="#">p. 297</a> )
D3	d3.xlarge   d3.2xlarge   d3.4xlarge   d3.8xlarge	Otimizada para armazenamento ( <a href="#">p. 297</a> )
D3en	d3en.large   d3en.xlarge   d3en.2xlarge   d3en.4xlarge   d3en.6xlarge   d3en.8xlarge   d3en.12xlarge	Otimizada para armazenamento ( <a href="#">p. 297</a> )
F1	f1.2xlarge   f1.4xlarge   f1.16xlarge	Computação acelerada ( <a href="#">p. 305</a> )
G3	g3s.xlarge   g3.4xlarge   g3.8xlarge   g3.16xlarge	Computação acelerada ( <a href="#">p. 305</a> )
G4ad	g4ad.xlarge   g4ad.2xlarge   g4ad.4xlarge   g4ad.8xlarge   g4ad.16xlarge	Computação acelerada ( <a href="#">p. 305</a> )
G4dn	g4dn.xlarge   g4dn.2xlarge   g4dn.4xlarge   g4dn.8xlarge   g4dn.12xlarge   g4dn.16xlarge   g4dn.metal	Computação acelerada ( <a href="#">p. 305</a> )
H1	h1.2xlarge   h1.4xlarge   h1.8xlarge   h1.16xlarge	Otimizada para armazenamento ( <a href="#">p. 297</a> )
I3	i3.large   i3.xlarge   i3.2xlarge   i3.4xlarge   i3.8xlarge   i3.16xlarge   i3.metal	Otimizada para armazenamento ( <a href="#">p. 297</a> )

Tipo	Sizes	Caso de uso
I3en	i3en.large   i3en.xlarge   i3en.2xlarge   i3en.3xlarge   i3en.6xlarge   i3en.12xlarge   i3en.24xlarge   i3en.metal	Otimizada para armazenamento (p. 297)
Inf1	inf1.xlarge   inf1.2xlarge   inf1.6xlarge   inf1.24xlarge	Computação acelerada (p. 305)
M4	m4.large   m4.xlarge   m4.2xlarge   m4.4xlarge   m4.10xlarge   m4.16xlarge	Propósito geral (p. 214)
M5	m5.large   m5.xlarge   m5.2xlarge   m5.4xlarge   m5.8xlarge   m5.12xlarge   m5.16xlarge   m5.24xlarge   m5.metal	Propósito geral (p. 214)
M5a	m5a.large   m5a.xlarge   m5a.2xlarge   m5a.4xlarge   m5a.8xlarge   m5a.12xlarge   m5a.16xlarge   m5a.24xlarge	Propósito geral (p. 214)
M5ad	m5ad.large   m5ad.xlarge   m5ad.2xlarge   m5ad.4xlarge   m5ad.8xlarge   m5ad.12xlarge   m5ad.16xlarge   m5ad.24xlarge	Propósito geral (p. 214)
M5d	m5d.large   m5d.xlarge   m5d.2xlarge   m5d.4xlarge   m5d.8xlarge   m5d.12xlarge   m5d.16xlarge   m5d.24xlarge   m5d.metal	Propósito geral (p. 214)
M5dn	m5dn.large   m5dn.xlarge   m5dn.2xlarge   m5dn.4xlarge   m5dn.8xlarge   m5dn.12xlarge   m5dn.16xlarge   m5dn.24xlarge   m5dn.metal	Propósito geral (p. 214)
M5n	m5n.large   m5n.xlarge   m5n.2xlarge   m5n.4xlarge   m5n.8xlarge   m5n.12xlarge   m5n.16xlarge   m5n.24xlarge   m5n.metal	Propósito geral (p. 214)
M5zn	m5zn.large   m5zn.xlarge   m5zn.2xlarge   m5zn.3xlarge   m5zn.6xlarge   m5zn.12xlarge   m5zn.metal	Propósito geral (p. 214)
M6g	m6g.medium   m6g.large   m6g.xlarge   m6g.2xlarge   m6g.4xlarge   m6g.8xlarge   m6g.12xlarge   m6g.16xlarge   m6g.metal	Propósito geral (p. 214)
M6gd	m6gd.medium   m6gd.large   m6gd.xlarge   m6gd.2xlarge   m6gd.4xlarge   m6gd.8xlarge   m6gd.12xlarge   m6gd.16xlarge   m6gd.metal	Propósito geral (p. 214)
M6i	m6i.large   m6i.xlarge   m6i.2xlarge   m6i.4xlarge   m6i.8xlarge   m6i.12xlarge   m6i.16xlarge   m6i.24xlarge   m6i.32xlarge	Propósito geral (p. 214)
Mac1	mac1.metal	Propósito geral (p. 214)
P2	p2.xlarge   p2.8xlarge   p2.16xlarge	Computação acelerada (p. 305)
P3	p3.2xlarge   p3.8xlarge   p3.16xlarge	Computação acelerada (p. 305)
P3dn	p3dn.24xlarge	Computação acelerada (p. 305)
P4d	p4d.24xlarge	Computação acelerada (p. 305)

Tipo	Sizes	Caso de uso
R4	r4.large   r4.xlarge   r4.2xlarge   r4.4xlarge   r4.8xlarge   r4.16xlarge	Otimizado para memória (p. 282)
R5	r5.large   r5.xlarge   r5.2xlarge   r5.4xlarge   r5.8xlarge   r5.12xlarge   r5.16xlarge   r5.24xlarge   r5.metal	Otimizado para memória (p. 282)
R5a	r5a.large   r5a.xlarge   r5a.2xlarge   r5a.4xlarge   r5a.8xlarge   r5a.12xlarge   r5a.16xlarge   r5a.24xlarge	Otimizado para memória (p. 282)
R5ad	r5ad.large   r5ad.xlarge   r5ad.2xlarge   r5ad.4xlarge   r5ad.8xlarge   r5ad.12xlarge   r5ad.16xlarge   r5ad.24xlarge	Otimizado para memória (p. 282)
R5b	r5b.large   r5b.xlarge   r5b.2xlarge   r5b.4xlarge   r5b.8xlarge   r5b.12xlarge   r5b.16xlarge   r5b.24xlarge   r5b.metal	Otimizado para memória (p. 282)
R5d	r5d.large   r5d.xlarge   r5d.2xlarge   r5d.4xlarge   r5d.8xlarge   r5d.12xlarge   r5d.16xlarge   r5d.24xlarge   r5d.metal	Otimizado para memória (p. 282)
R5dn	r5dn.large   r5dn.xlarge   r5dn.2xlarge   r5dn.4xlarge   r5dn.8xlarge   r5dn.12xlarge   r5dn.16xlarge   r5dn.24xlarge   r5dn.metal	Otimizado para memória (p. 282)
R5n	r5n.large   r5n.xlarge   r5n.2xlarge   r5n.4xlarge   r5n.8xlarge   r5n.12xlarge   r5n.16xlarge   r5n.24xlarge   r5n.metal	Otimizado para memória (p. 282)
R6g	r6g.medium   r6g.large   r6g.xlarge   r6g.2xlarge   r6g.4xlarge   r6g.8xlarge   r6g.12xlarge   r6g.16xlarge   r6g.metal	Otimizado para memória (p. 282)
R6gd	r6gd.medium   r6gd.large   r6gd.xlarge   r6gd.2xlarge   r6gd.4xlarge   r6gd.8xlarge   r6gd.12xlarge   r6gd.16xlarge   r6gd.metal	Otimizado para memória (p. 282)
T2	t2.nano   t2.micro   t2.small   t2.medium   t2.large   t2.xlarge   t2.2xlarge	Propósito geral (p. 214)
T3	t3.nano   t3.micro   t3.small   t3.medium   t3.large   t3.xlarge   t3.2xlarge	Propósito geral (p. 214)
T3a	t3a.nano   t3a.micro   t3a.small   t3a.medium   t3a.large   t3a.xlarge   t3a.2xlarge	Propósito geral (p. 214)
T4g	t4g.nano   t4g.micro   t4g.small   t4g.medium   t4g.large   t4g.xlarge   t4g.2xlarge	Propósito geral (p. 214)
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. 282)

Tipo	Sizes	Caso de uso
X1	x1.16xlarge   x1.32xlarge	Otimizado para memória (p. 282)
X1e	x1e.xlarge   x1e.2xlarge   x1e.4xlarge   x1e.8xlarge   x1e.16xlarge   x1e.32xlarge	Otimizado para memória (p. 282)
X2gd	x2gd.medium   x2gd.large   x2gd.xlarge   x2gd.2xlarge   x2gd.4xlarge   x2gd.8xlarge   x2gd.12xlarge   x2gd.16xlarge   x2gd.metal	Otimizado para memória (p. 282)
z1d	z1d.large   z1d.xlarge   z1d.2xlarge   z1d.3xlarge   z1d.6xlarge   z1d.12xlarge   z1d.metal	Otimizado para memória (p. 282)

## 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
A1	a1.medium   a1.large   a1.xlarge   a1.2xlarge   a1.4xlarge   a1.metal
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 \(p. 327\)](#).

#### 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.

## Tipos de virtualização de AMI

O tipo de virtualização da sua instância é determinado pela AMI usada para executá-la. Os tipos de instância da geração atual oferecem suporte apenas a HVM. Alguns tipos de instância de geração anterior são compatíveis com paravirtual (PV) e algumas regiões da AWS são compatíveis com as instâncias PV. Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#).

Para a melhor performance, recomendamos usar uma AMI HVM. Além disso, as AMIs HVM são necessárias para aproveitar as maiores capacidades de rede. A virtualização da HVM usa tecnologia assistida por hardware fornecida pela plataforma AWS. Com a virtualização da HVM, a VM guest é executada como se estivesse em uma plataforma de hardware nativa, exceto pelo fato de que ela ainda usa drivers de rede e armazenamento PV para melhorar a performance.

## 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: A1, C5, C5a, C5ad, C5d, C5n, C6g, C6gd, C6gn, D3, D3en, G4, I3en, Inf1, M5, M5a, M5ad, M5d, M5dn, M5n, M5zn, M6g, M6gd, M6i, p3dn.24xlarge, P4, R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6g, R6gd, T3, T3a, T4g, alta memória (u-\*), X2gd e z1d
- Bare metal: a1.metal, c5.metal, c5d.metal, c5n.metal, c6g.metal, c6gd.metal, i3.metal, i3en.metal, m5.metal, m5d.metal, m5dn.metal, m5n.metal, m5zn.metal, m6g.metal, m6gd.metal, mac1.metal, r5.metal, r5b.metal, r5d.metal, r5dn.metal, r5n.metal, r6g.metal, r6gd.metal, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal, x2gd.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 \(p. 1084\)](#).
  - 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 Linux \(p. 1015\)](#).
  - 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 \(p. 1096\)](#).

### 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 Linux \(p. 1434\)](#) e [Volumes SSD de NVMe \(p. 1508\)](#).
- 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 \(p. 1438\)](#).

## 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
C6g	Sim	Sim	Não	Sim	ENA
C6gd	Não	Sim	NVMe *	Sim	ENA
C6gn	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
Inf1	Sim	Sim	Não	Sim	ENA
M4	Sim	Não	Não	Sim	m4.16xlarge: ENA  Todos os outros tamanhos: Intel 82599 VF
M5	Sim	Sim	Não	Sim	ENA
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

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group	Redes avançadas
M5zn	Sim	Sim	Não	Sim	ENA
M6g	Sim	Sim	Não	Sim	ENA
M6gd	Não	Sim	NVMe *	Sim	ENA
M6i	Sim	Sim	Não	Sim	ENA
Mac1	Sim	Sim	Não	Não	ENA
P2	Sim	Não	Não	Sim	ENA
P3	Sim	Não	Não	Sim	ENA
P3dn	Não	Sim	NVMe *	Sim	ENA
P4d	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
R6g	Sim	Sim	Não	Sim	ENA
R6gd	Não	Sim	NVMe *	Sim	ENA
T2	Sim	Não	Não	Não	Não
T3	Sim	Sim	Não	Não	ENA
T3a	Sim	Sim	Não	Não	ENA
T4g	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
X2gd	Não	Sim	NVMe *	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 \(p. 1565\)](#).

## 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 às aplicações 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 M6g e M6gd

Essas instâncias são desenvolvidas pelos processadores AWS Graviton2 e fornecem computação, memória e rede balanceadas para uma grande variedade de workloads de uso geral. Elas são ideais para o seguinte:

- Servidores de aplicações
- Microsserviços
- Servidores de jogos
- Armazenamentos de dados de médio porte
- Frotas de cache

As instâncias bare metal, como a `m6g.metal`, fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória.

Para obter mais informações, consulte [Instâncias M6g do Amazon EC2](#).

#### 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 Mac1

Essas instâncias são alimentadas por minicomputadores Apple Mac. Elas fornecem até 10 Gbps de largura de banda de rede e largura de banda EBS de 8 Gbps através de conexões Thunderbolt 3 de alta velocidade. Elas são adequadas para desenvolver, criar, testar e assinar aplicações para dispositivos Apple, como iPhone, iPad, iPod, Mac, Apple Watch e Apple TV.

Para obter mais informações, consulte [Instâncias Mac do Amazon EC2 \(p. 264\)](#).

#### Instâncias T2, T3, T3a e T4g

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 \(p. 228\)](#). Elas são ideais para o seguinte:

- Sites e aplicações Web

- Reppositórios de códigos
- Ambientes de desenvolvimento, criação, teste e preparação
- Microsserviços

Para obter mais informações, consulte [Instância T2 do Amazon EC2](#), [Instâncias T3 do Amazon EC2](#) e [Instâncias T4g do Amazon EC2](#).

#### Tópicos

- [Especificações de hardware \(p. 216\)](#)
- [Da performance da instância \(p. 220\)](#)
- [Performance das redes \(p. 220\)](#)
- [Performance de E/S em SSD \(p. 224\)](#)
- [Recursos da instância \(p. 226\)](#)
- [Notas de release \(p. 227\)](#)
- [Instâncias expansíveis \(p. 228\)](#)
- [Instâncias Mac do Amazon EC2 \(p. 264\)](#)

## Especificações de hardware

Este é um resumo das especificações de hardware para instâncias de uso geral.

Tipo de instância	vCPUs padrão	Memória (GiB)
m4.large	2	8
m4.xlarge	4	16
m4.2xlarge	8	32
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Propósito geral

---

Tipo de instância	vCPUs padrão	Memória (GiB)
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Propósito geral

---

Tipo de instância	vCPUs padrão	Memória (GiB)
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
m6g.medium	1	4
m6g.large	2	8
m6g.xlarge	4	16
m6g.2xlarge	8	32
m6g.4xlarge	16	64
m6g.8xlarge	32	128
m6g.12xlarge	48	192
m6g.16xlarge	64	256
m6g.metal	64	256
m6gd.medium	1	4
m6gd.large	2	8
m6gd.xlarge	4	16
m6gd.2xlarge	8	32
m6gd.4xlarge	16	64

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Propósito geral

---

Tipo de instância	vCPUs padrão	Memória (GiB)
m6gd.8xlarge	32	128
m6gd.12xlarge	48	192
m6gd.16xlarge	64	256
m6gd.metal	64	256
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
mac1.metal	12	32
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

Tipo de instância	vCPUs padrão	Memória (GiB)
t3a.medium	2	4
t3a.large	2	8
t3a.xlarge	4	16
t3a.2xlarge	8	32
t4g.nano	2	0,5
t4g.micro	2	1
t4g.small	2	2
t4g.medium	2	4
t4g.large	2	8
t4g.xlarge	4	16
t4g.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 \(p. 616\)](#).

## 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 \(p. 1438\)](#).

Alguns tipos de instância de uso geral fornecem a capacidade de controlar os C-states e P-states do processador no Linux. Os C-states controlam os níveis de suspensão em que um núcleo pode entrar quando estiver inativo, enquanto os P-states controlam a performance desejada (em frequência da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para a instância do EC2 \(p. 604\)](#).

## 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 Linux \(p. 1015\)](#).

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   T4g	Até 5 Gbps †	<a href="#">ENA (p. 1016)</a>

Tipo de instância	Performance das redes	Redes avançadas
m4.large	Moderada	<a href="#">Intel 82599 VF (p. 1026)</a>
m4.xlarge   m4.2xlarge   m4.4xlarge	Alto	<a href="#">Intel 82599 VF (p. 1026)</a>
m5.4xlarge e menor   m5a.8xlarge e menor   m5ad.8xlarge e menor   m5d.4xlarge e menor   m6g.4xlarge e menor   m6gd.4xlarge e menor	Até 10 Gbps †	<a href="#">ENA (p. 1016)</a>
m4.10xlarge	10 Gbps	<a href="#">Intel 82599 VF (p. 1026)</a>
m5.8xlarge   m5.12xlarge   m5a.12xlarge   m5ad.12xlarge   m5d.8xlarge   m5d.12xlarge   mac1.metal	10 Gbps	<a href="#">ENA (p. 1016)</a>
m5a.16xlarge   m5ad.16xlarge   m6g.8xlarge   m6gd.8xlarge	12 Gbps	<a href="#">ENA (p. 1016)</a>
m6i.4xlarge e menor	Até 12,5 Gbps †	<a href="#">ENA (p. 1016)</a>
m6i.8xlarge	12,5 Gbps	<a href="#">ENA (p. 1016)</a>
m6i.12xlarge	18,75 Gbps	<a href="#">ENA (p. 1016)</a>
m5.16xlarge   m5a.24xlarge   m5ad.24xlarge   m5d.16xlarge   m6g.12xlarge   m6gd.12xlarge	20 Gbps	<a href="#">ENA (p. 1016)</a>
m5dn.4xlarge e menor   m5n.4xlarge e menor   m5zn.3xlarge e menor	Até 25 Gbps †	<a href="#">ENA (p. 1016)</a>
m4.16xlarge   m5.24xlarge   m5.metal   m5d.24xlarge   m5d.metal   m5dn.8xlarge   m5n.8xlarge   m6g.16xlarge   m6g.metal   m6gd.16xlarge   m6gd.metal   m6i.16xlarge	25 Gbps	<a href="#">ENA (p. 1016)</a>
m6i.24xlarge	37,5 Gbps	<a href="#">ENA (p. 1016)</a>
m5dn.12xlarge   m5n.12xlarge   m5zn.6xlarge   m6i.32xlarge	50 Gbps	<a href="#">ENA (p. 1016)</a>
m5dn.16xlarge   m5n.16xlarge	75 Gbps	<a href="#">ENA (p. 1016)</a>

Tipo de instância	Performance das redes	Redes avançadas
m5dn.24xlarge   m5dn.metal   m5n.24xlarge   m5n.metal   m5zn.12xlarge   m5zn.metal	100 Gbps	<a href="#">ENA (p. 1016)</a> , <a href="#">EFA (p. 1044)</a>

† 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 \(p. 1013\)](#).

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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Propósito geral

---

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
m5zn.large	3	25
m5zn.xlarge	5	25
m5zn.2xlarge	10	25
m5zn.3xlarge	15	25
m6g.medium	5.	10
m6g.large	.75	10
m6g.xlarge	1.25	10
m6g.2xlarge	2,5	10
m6g.4xlarge	5	10
m6gd.medium	5.	10
m6gd.large	.75	10
m6gd.xlarge	1.25	10
m6gd.2xlarge	2,5	10
m6gd.4xlarge	5	10
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
t4g.nano	.032	5
t4g.micro	.064	5
t4g.small	.128	5
t4g.medium	.256	5
t4g.large	.512	5
t4g.xlarge	1.024	5
t4g.2xlarge	2.048	5

## Performance de E/S em SSD

Se você usar a AMI do Linux com kernel versão 4.4 ou superior e 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

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
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
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
m6gd.medium	13.438	5.625
m6gd.large	26.875	11.250
m6gd.xlarge	53.750	22.500
m6gd.2xlarge	107.500	45.000
m6gd.4xlarge	215.000	90.000
m6gd.8xlarge	430.000	180.000
m6gd.12xlarge	645.000	270.000
m6gd.16xlarge	860.000	360.000
m6gd.metal	860.000	360.000

\* 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 \(p. 1510\)](#).

## 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
M5n	Sim	Sim	Não	Sim
M5zn	Sim	Sim	Não	Sim
M6g	Sim	Sim	Não	Sim
M6gd	Não	Sim	NVMe *	Sim
M6i	Sim	Sim	Não	Sim
Mac1	Sim	Sim	Não	Não
T2	Sim	Não	Não	Não
T3	Sim	Sim	Não	Não
T3a	Sim	Sim	Não	Não
T4g	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 Linux \(p. 1434\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1494\)](#)
- [Grupos de posicionamento \(p. 1084\)](#)

## 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 M6g e M6gd têm um processador AWS Graviton2 baseado na arquitetura Arm de 64 bits.
- 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).
- As instâncias Mac1 possuem um processador Intel de oitava geração (Coffee Lake) Core i7 de 3,2 GHz.
- As instâncias T4g têm um processador AWS Graviton2 baseado na arquitetura Arm de 64 bits.
- Instâncias criadas no [Sistema Nitro \(p. 210\)](#), 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 \(p. 210\)](#) têm os seguintes requisitos:
  - Os [drivers de NVMe \(p. 1434\)](#) devem estar instalados
  - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1016\)](#) devem estar instalados

As AMIs do Linux a seguir atendem a esses requisitos:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (com kernel linux-aws) ou posterior
- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior
- As instâncias com [processador AWS Graviton](#) têm os seguintes requisitos:
  - Use uma AMI para a arquitetura Arm de 64 bits.
  - Suporte à inicialização por meio de UEFI com tabelas de ACPI e oferecer suporte a hot-plug ACPI ou a dispositivos PCI.

As seguintes AMIs do Linux atendem a esses requisitos:

- Amazon Linux 2 (Arm de 64 bits)
- Ubuntu 16.04 ou posterior (Arm de 64 bits)
- Red Hat Enterprise Linux 8.0 ou posterior (Arm de 64 bits)
- SUSE Linux Enterprise Server 15 ou posterior (Arm de 64 bits)
- Debian 10 ou posterior (Arm de 64 bits)
- Para obter a melhor performance de suas instâncias M6i, certifique-se de que elas tenham o driver ENA versão 2.2.9 ou posterior. Usar um driver ENA anterior à versão 1.2 com essas instâncias causará falhas no anexo da interface de rede. As AMIs a seguir têm driver ENA compatível.
  - Amazon Linux 2 com kernel 4.14.186
  - Ubuntu 20.04 com kernel 5.4.0-1025-aws
  - Red Hat Enterprise Linux 8.3 com kernel 4.18.0-240.1.1.el8\_3.arch
- SUSE Linux Enterprise Server 15 SP2 com Kernel 5.3.18-24.15.1

- As instâncias do Amazon EC2 Mac são compatíveis com o macOS Mojave (versão 10.14), macOS Catalina (versão 10.15) e macOS Big Sur (versão 11).
- 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 \(p. 1520\)](#).
- 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. O Amazon Linux 2 e as versões mais recentes da AMI do Amazon Linux são compatíveis com PCIe hotplug nativo, mas as versões anteriores não são. Você precisa ativar as seguintes opções de configuração do kernel do Linux:

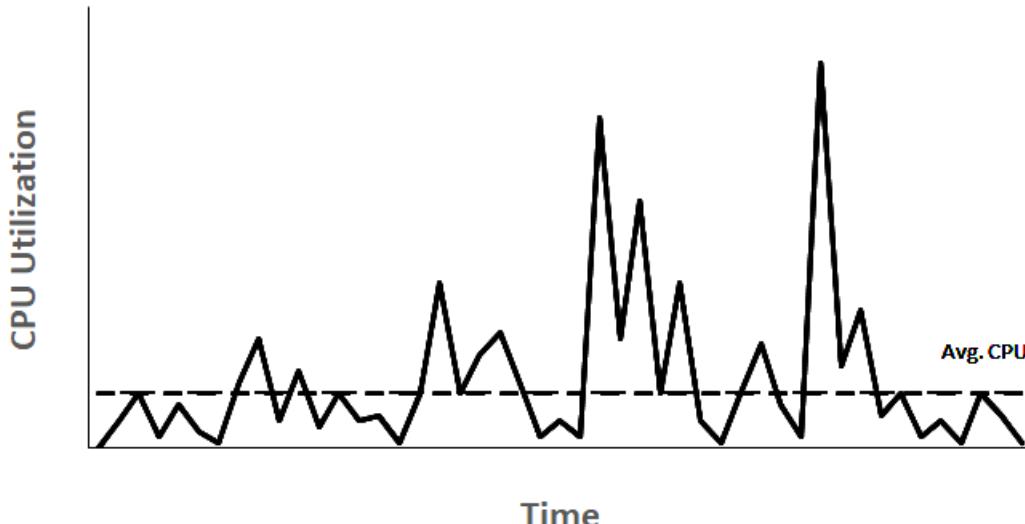
```
CONFIG_HOTPLUG_PCI_PCIE=y  
CONFIG_PCIEASPM=y
```

- 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 criadas no Sistema Nitro devem ter system-logind ou acpid instalado para oferecer suporte ao desligamento normal por meio de solicitações de API.
- 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 T4g, 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 \(p. 338\)](#).

Tópicos

- [Práticas recomendadas \(p. 230\)](#)
- [Principais conceitos e definições para instâncias expansíveis \(p. 230\)](#)
- [Modo ilimitado de instâncias expansíveis \(p. 237\)](#)
- [Modo padrão de instâncias expansíveis \(p. 245\)](#)
- [Trabalhar com instâncias expansíveis \(p. 255\)](#)
- [Monitorar seus créditos da CPU \(p. 261\)](#)

## 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 \(p. 227\)](#).

## 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 menores 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 exceder 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 \(p. 231\)](#)
- [Ganhe créditos de CPU \(p. 234\)](#)
- [Taxa de ganhos de créditos de CPU \(p. 235\)](#)
- [Limite de acúmulo de créditos de CPU \(p. 235\)](#)
- [Duração dos créditos de CPU acumulados \(p. 236\)](#)
- [Utilização da linha de base \(p. 236\)](#)

#### [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 \(p. 888\)](#).

#### 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 vCPUs \* 5% da linha de base \* 60 minutos = 6 créditos por hora

#### Créditos gastos ou usados

Créditos usados continuamente por uma instância quando ela está em execução.

Créditos de CPU gastos por minuto = Número de vCPUs \* utilização da CPU \* 1 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:

Créditos de CPU acumulados = (Créditos obtidos por hora - Créditos usados por hora) = 6 - 2 vCPUs \* 2% de utilização da CPU \* 60 minutos = 6 - 2,4 = 3,6 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
<strong>Última geração</strong>			
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)
<strong>Geração anterior</strong>			
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				

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
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%**
T4g				
t4g.nano	6	144	2	5%**
t4g.micro	12	288	2	10%**
t4g.small	24	576	2	20%**
t4g.medium	24	576	2	20%**
t4g.large	36	864	2	30%**
t4g.xlarge	96	2304	4	40%**
t4g.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 \(p. 236\)](#).

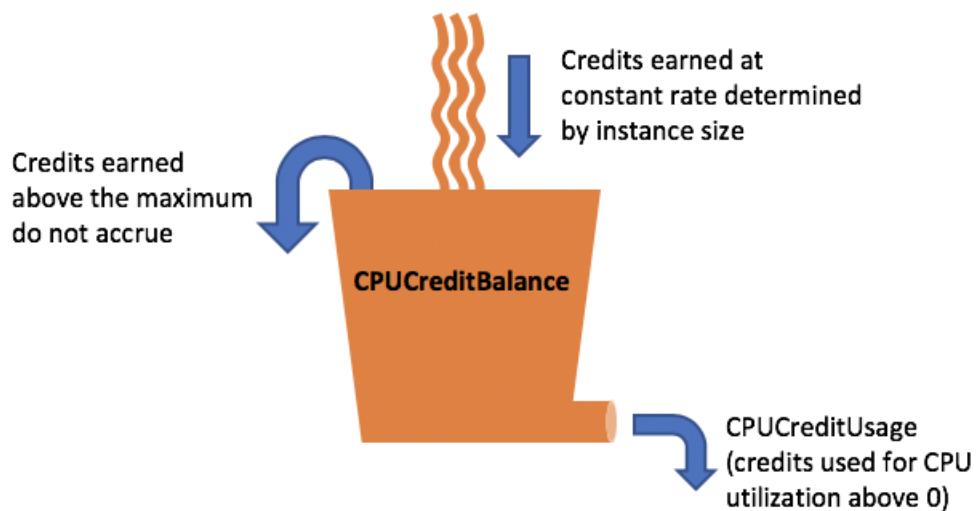
\*\*\* Cada vCPU é uma thread de um núcleo Intel Xeon ou de um núcleo AMD EPYC, exceto para instâncias T2 e T4g.

### 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.

### Limite 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 cheio 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 de 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 \(p. 246\)](#).

As instâncias T4g, 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 de `>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 T4g, 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 `CPUCreditBalance` na [Tabela de métricas do CloudWatch \(p. 261\)](#).

### 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:

$(\text{number of credits earned}/\text{number of vCPUs})/60 \text{ minutes} = \% \text{ baseline utilization}$

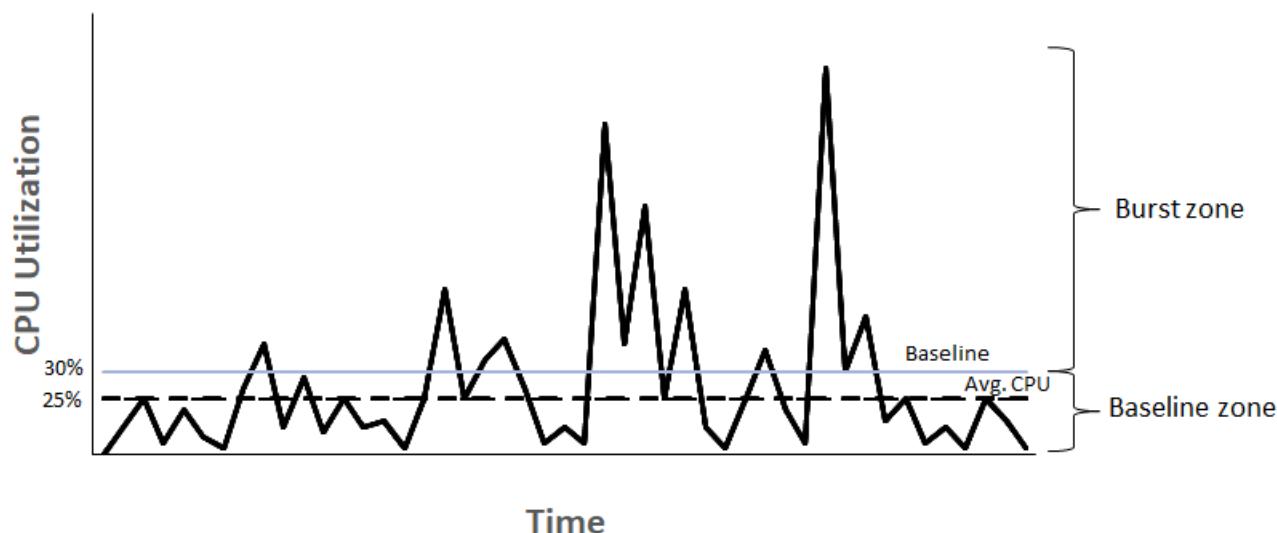
Por exemplo, uma instância t3.nano, com 2 vCPUs, ganha 6 créditos por hora, resultando em uma utilização de linha de base de 5%, que é calculada da seguinte forma:

$(6 \text{ credits earned}/2 \text{ vCPUs})/60 \text{ minutes} = 5\% \text{ baseline utilization}$

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 \(p. 236\)](#) da instância.

As instâncias T4g, 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 \(p. 245\)](#) para evitar custos mais altos. Para obter mais informações, consulte [Os créditos excedentes podem gerar cobranças \(p. 241\)](#) e [Instâncias expansíveis \(p. 439\)](#).

## 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 \(p. 238\)](#)
  - Como funcionam as instâncias expansíveis (p. 238)
  - Quando usar o modo ilimitado versus CPU fixa (p. 239)
  - Os créditos excedentes podem gerar cobranças (p. 241)
  - Nenhum crédito de execução para T2 ilimitada (p. 241)
  - Ativar modo ilimitado (p. 241)
  - O que acontece com os créditos quando é feita alternância de ilimitada para padrão (p. 242)
  - Monitorar uso de crédito (p. 242)
- [Exemplos de modo ilimitado \(p. 242\)](#)
  - Exemplo 1: explicar o uso de créditos com T3 ilimitada (p. 242)
  - Exemplo 2: explicar o uso de créditos com T2 ilimitada (p. 243)

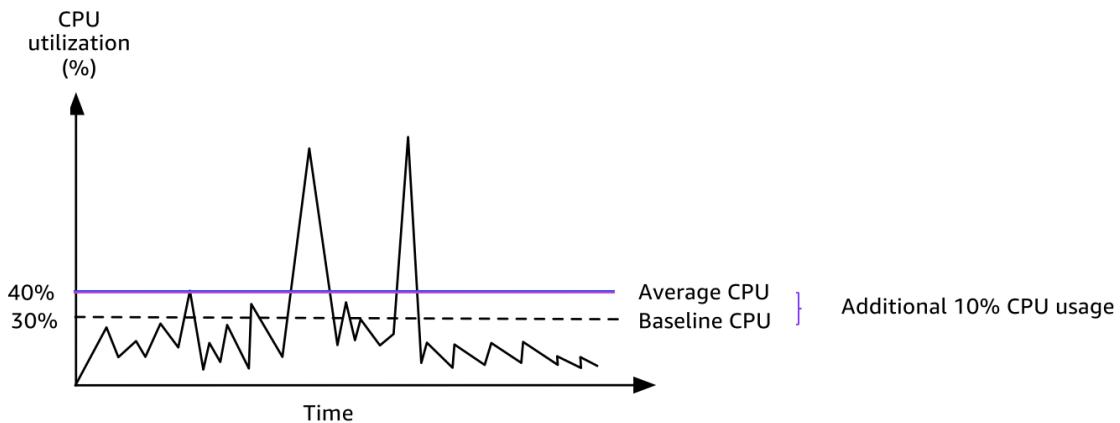
## [Conceitos do modo ilimitado](#)

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 \(p. 236\)](#). 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.



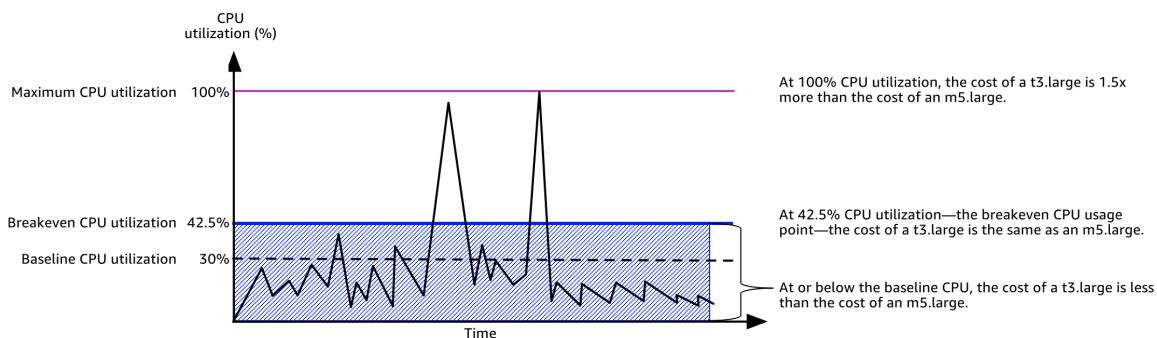
Para obter mais informações sobre a utilização da linha de base por vCPU para cada tipo de instância e quantos créditos cada tipo de instância recebe, consulte a [tabela de créditos \(p. 234\)](#).

#### 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 de vCPU	Cobrança por hora de vCPU	Cobrança por minuto de vCPU	Mais minutos de uso adicional de vCPU	% de CPU de intermitência	% de CPU disponível			
									F	G	H = G / 60	I = E / H	J = (I / 60) / B
				(%)									
t3.large	2	US\$ 0,096 USD 0,0835	US\$ 0,125 USD	30%		0,05 USD	US\$ 0,000833	15	12,5%	42,5%			

\*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%

Tipo de instância do T3	Uso da CPU de equilíbrio (em %) para T3 comparado a M5
t3.xlarge	52,5 %
t3.2xlarge	52,5 %

### Os créditos excedentes podem gerar cobranças

Se a utilização média de CPU de um实例 for igual ou inferior à linha de base, a实例 não incorrerá em encargos adicionais. Como uma实例 ganha um [número máximo de créditos \(p. 234\)](#) em um período de 24 horas (por exemplo, uma实例 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 cobrança imediatamente.

Contudo, se a utilização de CPU permanecer acima da linha de base, a实例 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 \(p. 234\)](#) que a实例 pode obter em um período de 24 horas. Os créditos excedentes gastos acima do limite máximo são cobrados no final da hora.
- A实例 é interrompida ou encerrada.
- A实例 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 \(p. 261\)](#).

### Nenhum crédito de execução para T2 ilimitada

As instâncias T2 padrão recebem [créditos de execução \(p. 246\)](#), mas as instâncias T2 ilimitadas não as recebem. Uma实例 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实例 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 T4g, 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实例 interrompida ou em execução. Para obter mais informações, consulte [Iniciar uma instância expansível como ilimitada ou padrão \(p. 255\)](#) e [Modificar a especificação de crédito de uma instância expansível \(p. 258\)](#).

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 expansíveis na conta sejam executadas usando a opção de crédito padrão. Para obter mais informações, consulte [Definir a especificação de crédito padrão para a conta \(p. 260\)](#).

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 \(p. 257\)](#) e [Visualizar a especificação de crédito padrão \(p. 260\)](#).

### 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 \(p. 261\)](#).

### 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 \(p. 242\)](#)
- [Exemplo 2: explicar o uso de créditos com T2 ilimitada \(p. 243\)](#)

#### 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.

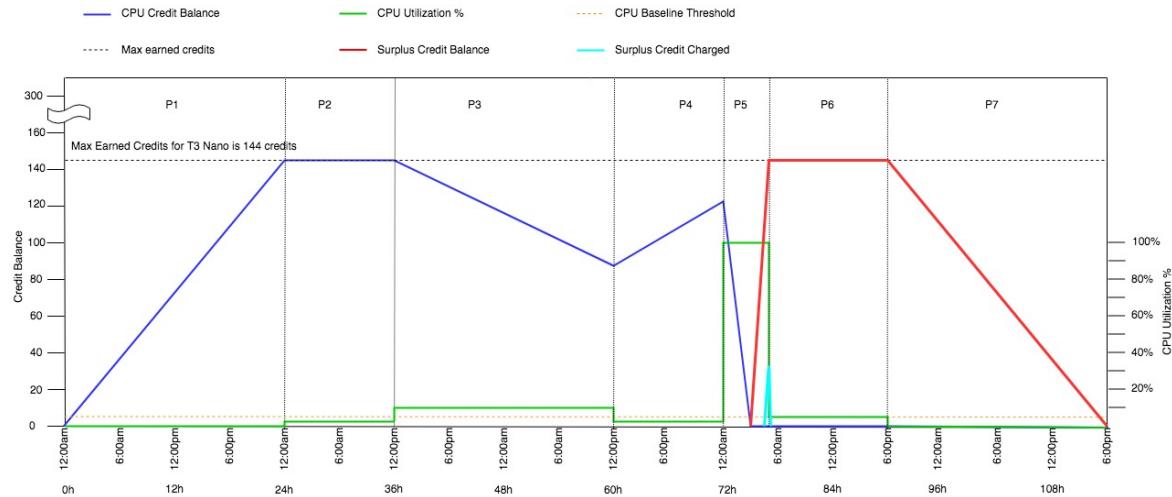
P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor `CPUCreditBalance` diminui para 86,4 créditos.

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:

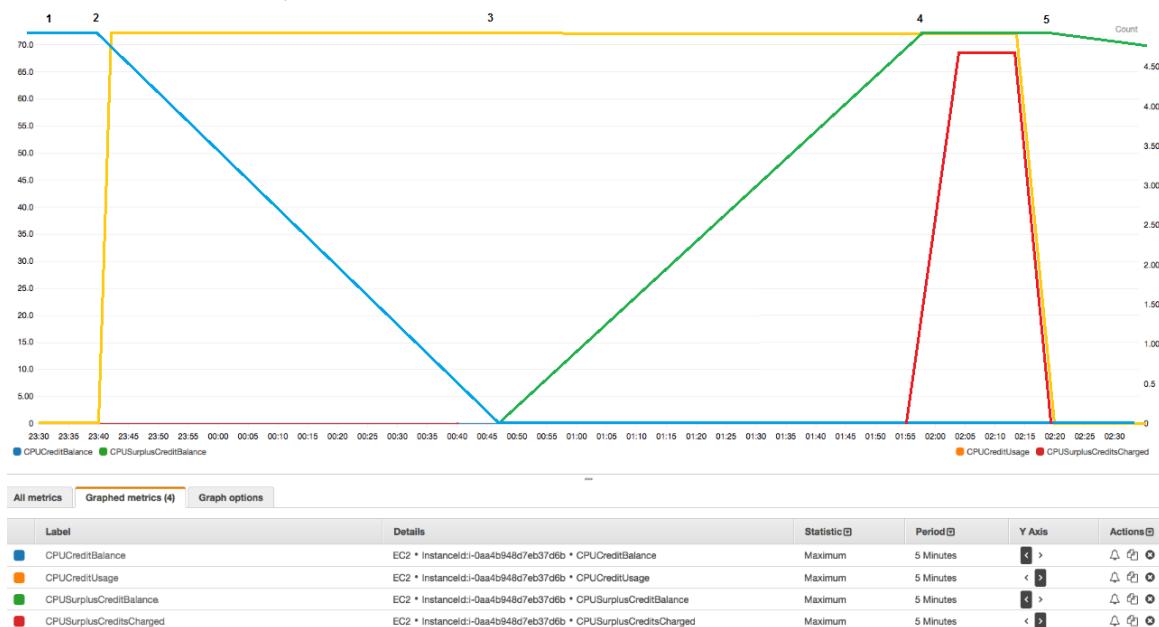
1 – Nos primeiros 10 minutos, `CPUCreditUsage` está em 0 e o valor `CPUCreditBalance` permanece no limite máximo de 72.

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 às 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 0,05 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  $0,42 \text{ hora de vCPU} \times 0,05 \text{ USD/hora de vCPU} = 0,021 \text{ USD}$ , arredondado para 0,02 USD.

Esta é a conta de final do mês desta instância T2 ilimitada:

Amazon Elastic Compute Cloud running Linux/UNIX			
\$0.0058 per On Demand Linux t2.nano Instance Hour		720.000 Hrs	\$4.18
Amazon Elastic Compute Cloud T2 CPU Credits			
\$0.05 per vCPU-Hour of T2 CPU credits		0.420 vCPU-Hours	\$0.02

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 \(p. 230\)](#).

### Tópicos

- [Conceitos do modo padrão \(p. 245\)](#)
  - Como funcionam as instâncias expansíveis padrão (p. 245)
  - Créditos de execução (p. 246)
  - Limites de crédito de execução (p. 246)
  - Diferenças entre créditos de execução e créditos ganhos (p. 247)
- [Exemplos de modo padrão \(p. 247\)](#)
  - Exemplo 1: explicar o uso de créditos com T3 padrão (p. 248)
  - Exemplo 2: explicar o uso de créditos com T2 padrão (p. 249)
    - Período 1: 1 a 24 horas (p. 249)
    - Período 2: 25 a 36 horas (p. 250)
    - Período 3: 37 a 61 horas (p. 251)
    - Período 4: 62 a 72 horas (p. 252)
    - Período 5: 73 a– 75 horas (p. 252)
    - Período 6: 76 a 90 horas (p. 253)
    - Período 7: 91 a 96 horas (p. 254)

### [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 T4g, 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 startup. 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 T4g, 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 \(p. 234\)](#).

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
<code>t1.micro</code>	15	1
<code>t2.nano</code>	30	1
<code>t2.micro</code>	30	1
<code>t2.small</code>	30	1
<code>t2.medium</code>	60	2
<code>t2.large</code>	60	2
<code>t2.xlarge</code>	120	4
<code>t2.2xlarge</code>	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 \(p. 237\)](#) 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	<p>As instâncias T2 padrão recebem 30 créditos de execução por vCPU na execução ou inicialização.</p> <p>Se uma instância T2 for alterada de <code>unlimited</code> para <code>standard</code>, ela não obtém créditos de execução no momento em que é alterada.</p>	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 <a href="#">Tabela de créditos (p. 234)</a> .
Limite de ganho de crédito	O limite para receber créditos de execução é de 100 execuções ou inicializações de todas as instâncias T2 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.	Uma instância T2 não pode acumular mais créditos do que o limite de saldo de crédito de CPU. Se o saldo de créditos 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 <a href="#">Tabela de créditos (p. 234)</a> .
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 \(p. 261\)](#).

### 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 \(p. 248\)](#)
- [Exemplo 2: explicar o uso de créditos com T2 padrão \(p. 249\)](#)

### [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 \(p. 234\)](#).

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.

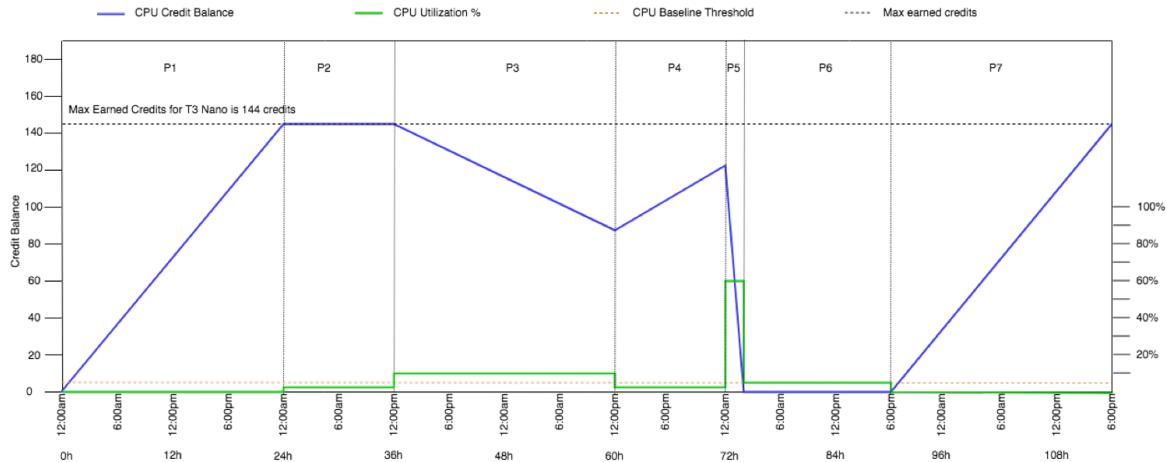
P3 – nas próximas 24 horas, a utilização de CPU é de 7% (acima da linha de base), o que exige um gasto de 57,6 créditos. A instância gasta mais do que ganha, e o valor CPUCreditBalance diminui para 86,4 créditos.

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 intermitênciam 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.

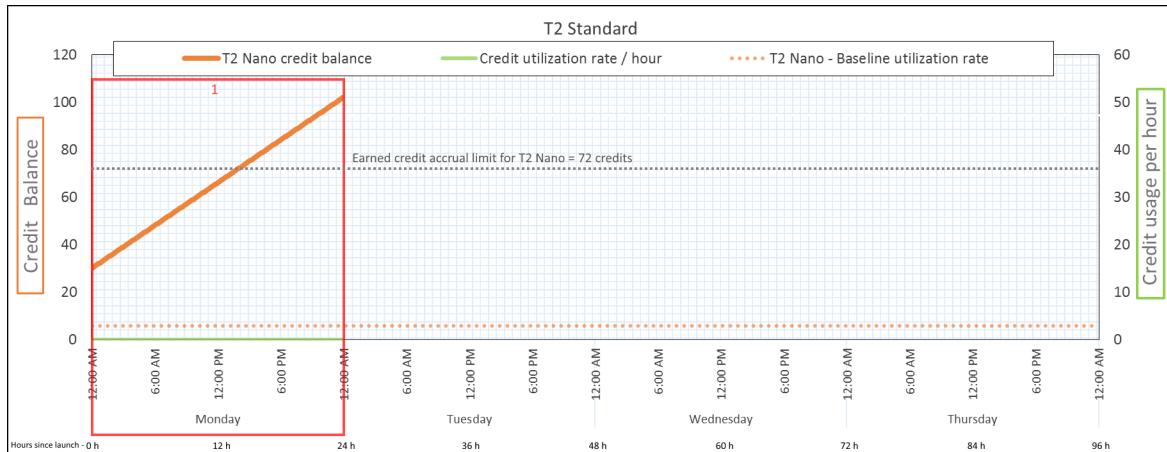
A instância `t2.nano` obtém 30 créditos de execução quando é executada e ganha 72 créditos a cada 24 horas. Seu limite de saldo é de 72 créditos ganhos. Os créditos de execução não são considerados no limite. Assim que o limite é atingido, os novos créditos ganhos são descartados. Para obter mais informações sobre o número de créditos que podem ser ganhos e acumulados, consulte a [Tabela de créditos \(p. 234\)](#). Para obter mais informações sobre limites, consulte [Limites de crédito de execução \(p. 246\)](#).

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)

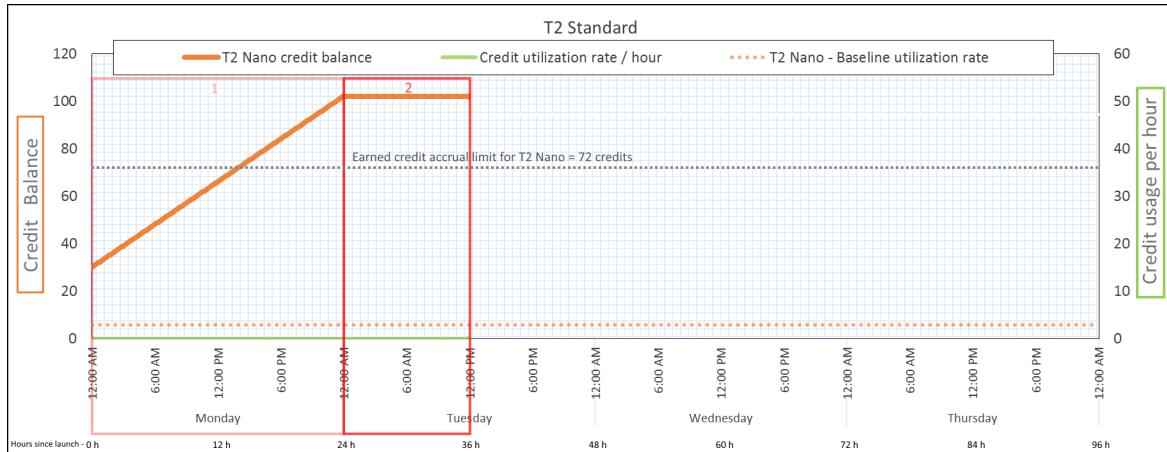
### Conclusion

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)
--------------------------	---

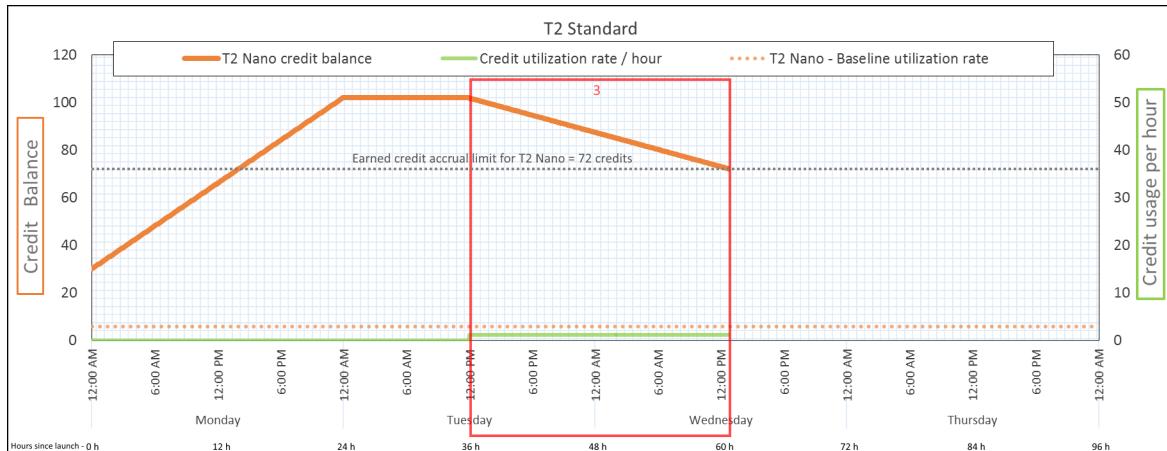
Taxa de ganhos de crédito	72 créditos por 24 horas (3 créditos por hora)
Taxa de descarte de crédito	72 créditos por 24 horas (100% de taxa de ganhos de crédito)
Saldo de crédito	102 créditos (30 créditos de execução + 72 créditos ganhos) – o saldo não é alterado

### 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 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 diminuir. 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)

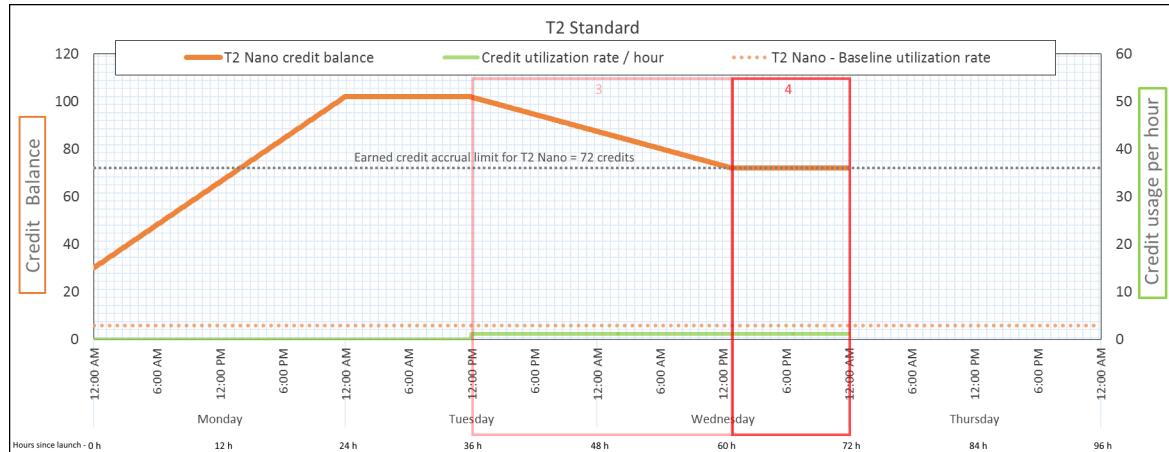
### Conclusion

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.



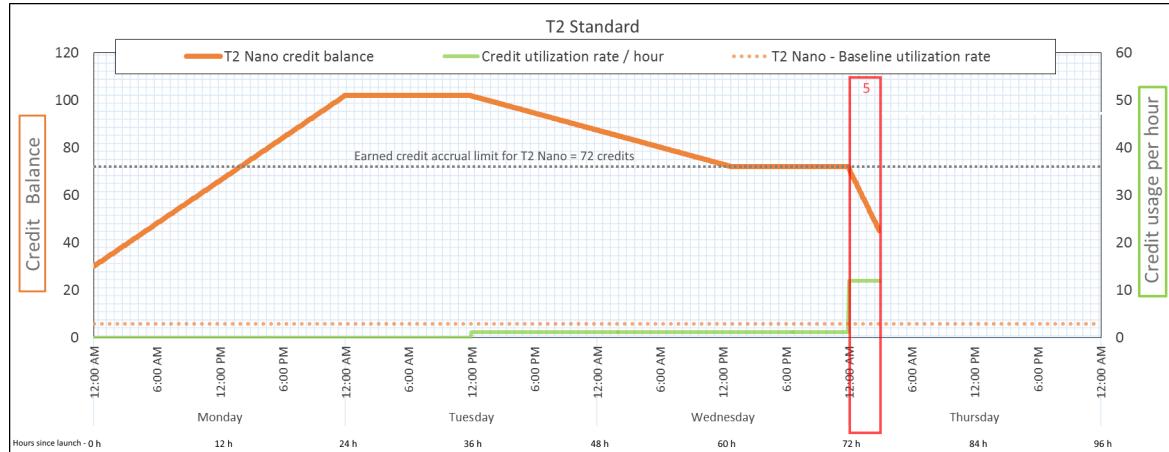
Taxa de gasto de crédito	28,8 créditos por 24 horas (1,2 créditos por hora, 2% de utilização da CPU, 40% de taxa de ganhos de crédito) – 13,2 —créditos em 11 horas
Taxa de ganhos de crédito	72 créditos por 24 horas
Taxa de descarte de crédito	43,2 créditos por 24 horas (60% de taxa de ganhos de crédito)
Saldo de crédito	72 créditos (0 créditos de execução, 72 créditos ganhos) – 0 —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 diminuiu 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

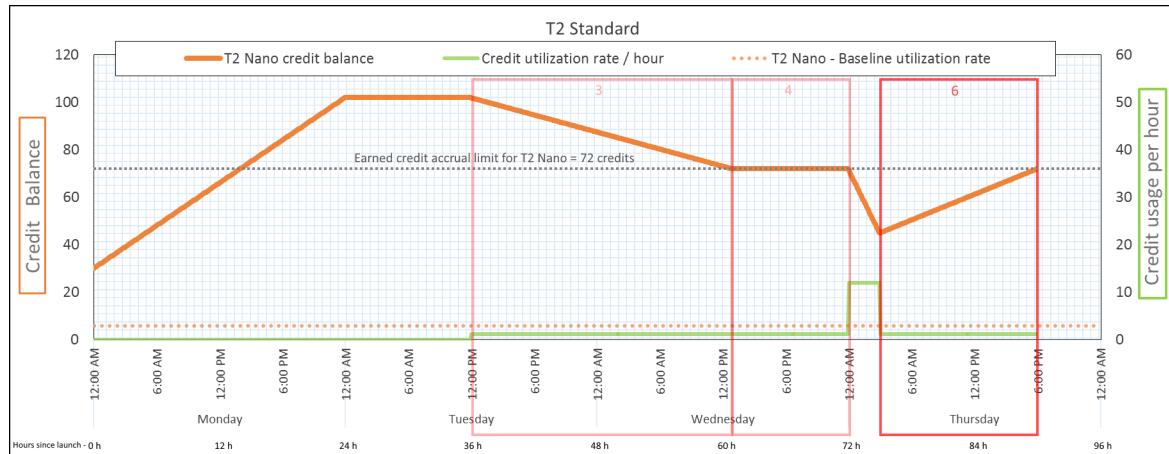
Se uma instância gastar mais créditos do que ganhar, seu balanço diminuirá.

### 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)

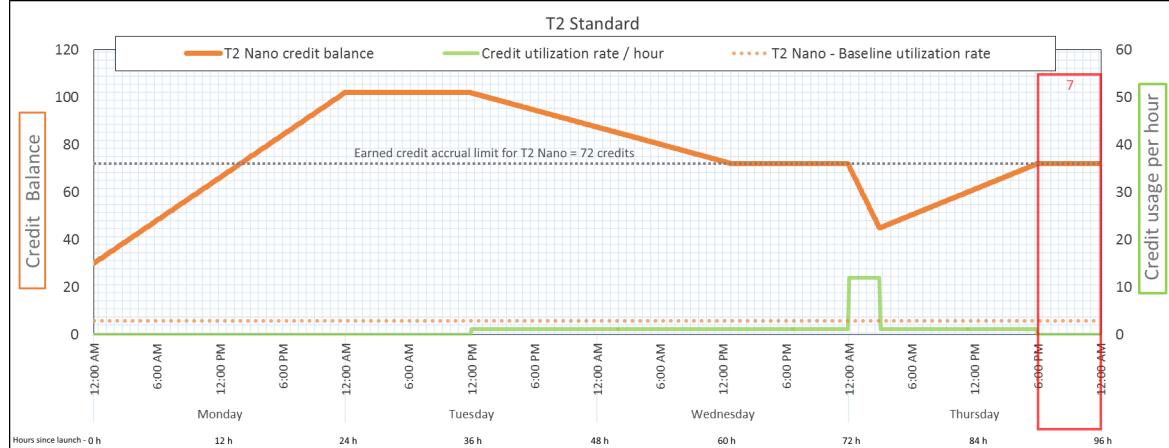
## Conclusion

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 \(p. 234\)](#).

## 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 T4g, 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 \(p. 255\)](#)
- [Usar um grupo de Auto Scaling para executar uma instância expansível como ilimitada \(p. 256\)](#)
- [Exibir a especificação de crédito de uma instância expansível \(p. 257\)](#)
- [Modificar a especificação de crédito de uma instância expansível \(p. 258\)](#)
- [Definir a especificação de crédito padrão para a conta \(p. 260\)](#)
- [Visualizar a especificação de crédito padrão \(p. 260\)](#)

### 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 \(p. 256\)](#).

### Requirements

- Você deve executar as instâncias usando um volume do Amazon EBS como o dispositivo raiz. Para obter mais informações, consulte [Volume do dispositivo raiz da instância do Amazon EC2 \(p. 1521\)](#).
- Para obter mais informações sobre os requisitos de driver de AMI para essas instâncias, consulte [Notas de release \(p. 227\)](#).

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. \(p. 510\)](#).

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 T4g, 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. \(p. 510\)](#).

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 T4g, 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 T4g, 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 \(p. 261\)](#)
- [Calcular o uso de crédito da CPU \(p. 262\)](#)

### 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 \(p. 234\)](#) 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 \(p. 875\)](#).

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 T4g, 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"> <li>• 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.</li> <li>• A instância é interrompida ou encerrada.</li> <li>• A instância é alterada de <code>unlimited</code> para <code>standard</code>.</li> </ul> <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 \(p. 234\)](#).

**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 \(p. 234\)](#) 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 \(p. 234\)](#) 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 Mac do Amazon EC2

As instâncias Mac1 suportam nativamente o sistema operacional macOS. Elas são criadas em hardware Mac mini e baseadas em processadores Intel de oitava geração (Coffee Lake) Core i7 de 3,2 GHz. Essas instâncias são ideais para desenvolver, criar, testar e assinar aplicações para dispositivos Apple, como iPhone, iPad, iPod, Mac, Apple Watch e Apple TV. Você pode se conectar à instância do Mac usando SSH ou Apple Remote Desktop (ARD).

Para obter mais informações, consulte [Instâncias Mac do Amazon EC2 e Preços](#).

#### Tópicos

- [Considerations \(p. 265\)](#)
- [Executar uma instância Mac usando o console \(p. 266\)](#)
- [Executar uma instância Mac usando o AWS CLI \(p. 266\)](#)
- [Conectar-se à instância usando SSH \(p. 267\)](#)
- [Conecte-se à instância usando o Apple Remote Desktop \(p. 268\)](#)

- [Modificar a resolução de tela do macOS em instâncias Mac \(p. 268\)](#)
- [AMIs do macOS do EC2 \(p. 269\)](#)
- [Atualizar o sistema operacional e o software \(p. 269\)](#)
- [EC2 MacOS Init \(p. 270\)](#)
- [Monitoramento do EC2 System para macOS \(p. 270\)](#)
- [Aumente o tamanho de um volume do EBS na instância do Mac \(p. 271\)](#)
- [Interromper e encerrar a instância do Mac \(p. 271\)](#)
- [Assinar notificações de AMI do macOS \(p. 272\)](#)
- [Libere o Host dedicado para a sua instância do Mac \(p. 273\)](#)

## Considerations

As seguintes considerações se aplicam às instâncias do Mac:

- As instâncias Mac só estão disponíveis como instâncias bare metal em [hosts dedicados \(p. 440\)](#), com um período mínimo de alocação de 24 horas antes de você poder liberar o host dedicado. Você pode executar uma instância Mac por Host dedicado. Você pode compartilhar o Host dedicado com as contas da AWS ou com unidades organizacionais dentro da sua organização de AWS ou toda a organização da AWS.
- As instâncias Mac estão disponíveis apenas como Instâncias on-demand. Elas não estão disponíveis como Instâncias spot ou Instâncias reservadas. Você pode economizar dinheiro em instâncias Mac comprando um [Savings Plan](#).
- As instâncias Mac podem executar um dos seguintes sistemas operacionais:
  - macOS Catalina (versão 10.15)
  - macOS Mojave (versão 10.14)
  - macOS Big Sur (versão 11)
- Se você anexar um volume do EBS a uma instância Mac em execução, será necessário reiniciar a instância para disponibilizar o volume.
- Se você redimensionou um volume do EBS existente em uma instância Mac em execução, será necessário reiniciar a instância para disponibilizar o novo tamanho.
- Se você anexar uma interface de rede a uma instância Mac em execução, será necessário reiniciar a instância para disponibilizar a interface de rede.
- AWS não gerencia nem oferece suporte ao SSD interno no hardware Apple. É altamente recomendável, em vez disso, o uso de volumes do Amazon EBS. Os volumes do EBS oferecem os mesmos benefícios de elasticidade, disponibilidade e durabilidade em instâncias Mac como em qualquer outra instância do EC2.
- Recomendamos o uso de SSD de uso geral (gp2 e gp3) e SSD de IOPS provisionadas (io1 e io2) com instâncias Mac para obter a performance ideal do EBS.
- Não é possível usar instâncias do Mac com Amazon EC2 Auto Scaling.
- As atualizações automáticas de software estão desativadas. Recomendamos que você aplique as atualizações e as teste na sua instância antes de colocá-la em produção. Para obter mais informações, consulte [Atualizar o sistema operacional e o software \(p. 269\)](#).
- Quando você interrompe ou encerra uma instância do Mac, um fluxo de trabalho de depuração é executado no Host dedicado. Para obter mais informações, consulte [Interromper e encerrar a instância do Mac \(p. 271\)](#).
- Warning

Não use o FileVault. Se forem necessários dados em repouso e dados em trânsito, use [criptografia do EBS](#) para evitar problemas de inicialização e impacto na performance. Ativar o FileVault fará com que o host não seja inicializado devido ao bloqueio das partições.

## Executar uma instância Mac usando o console

Você pode executar uma instância Mac usando o AWS Management Console, conforme descrito no procedimento a seguir As instâncias Mac exigem um [host dedicado](#) (p. 440).

Para executar uma instância Mac em 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. Escolha Allocate (Alocar) Host dedicado e, em seguida, faça o seguinte:
  - a. Para a família de instâncias, escolha **mac1**. Se **mac1** não aparecer na lista, significa que ele não recebe suporte na região selecionada no momento.
  - b. Em Instance Type (Tipo de instância), selecione **mac1.metal**.
  - c. Em Availability Zone (Zona de disponibilidade), selecione a zona de disponibilidade do Host dedicado.
  - d. Para a Quantity (Quantidade), mantenha **1**.
  - e. Escolha Allocate.
4. Selecione o Host dedicado que você criou e, em seguida, faça o seguinte:
  - a. Escolha Actions (Ações), Launch instances onto host (Executar instâncias no host).
  - b. Selecione uma AMI do macOS.
  - c. Selecione o tipo de instância do **mac1.metal**.
  - d. Na página Configurar Detalhes da Instância (Configurar detalhes da instância), verifique se a Tenancy (Locação) e o Host estão pré-configurados com base no Host dedicado que você criou. Atualize Affinity (Afinidade) conforme necessário.
  - e. Conclua o assistente, especificando os volumes, grupos de segurança e pares de chaves do EBS conforme necessário.
5. Uma página de confirmação informa que sua instância está sendo executada. Selecione Visualizar instâncias para fechar a página de confirmação e voltar ao console. O estado inicial de uma instância é **pending**. A instância está pronta quando seu estado muda para **running** e passa verificações de status.

## Executar uma instância Mac usando o AWS CLI

Use o comando [alocar-hosts](#) para alocar uma Host dedicado para a instância do Mac.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-zone us-east-1b --auto-placement "on" --quantity 1
```

Use o comando [run-instances](#) para executar uma instância do Mac.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement Tenancy=host --image-id ami_id --key-name my-key-pair
```

O estado inicial de uma instância é **pending**. A instância está pronta quando seu estado muda para **running** e passa verificações de status. Use o comando [describe-instance-status](#) para exibir informações de status para a instância:

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Veja a seguir um exemplo de saída para uma instância que está sendo executada e passou por verificações de status.

```
{  
    "InstanceStatuses": [  
        {  
            "AvailabilityZone": "us-east-1b",  
            "InstanceId": "i-017f8354e2dc69c4f",  
            "InstanceState": {  
                "Code": 16,  
                "Name": "running"  
            },  
            "InstanceStatus": {  
                "Details": [  
                    {  
                        "Name": "reachability",  
                        "Status": "passed"  
                    }  
                ],  
                "Status": "ok"  
            },  
            "SystemStatus": {  
                "Details": [  
                    {  
                        "Name": "reachability",  
                        "Status": "passed"  
                    }  
                ],  
                "Status": "ok"  
            }  
        }  
    ]  
}
```

## Conectar-se à instância usando SSH

Por padrão, as instâncias Mac do Amazon EC2 não permitem SSH de raiz remota. A autenticação com senha é desabilitada para evitar ataques de força bruta em senhas. A conta ec2-user é configurada para login remoto usando SSH. A conta ec2-user também tem privilégios de sudo. Depois de se conectar à instância, você pode adicionar outros usuários.

Para oferecer suporte à conexão com a instância usando SSH, execute a instância usando um par de chaves e um grupo de segurança que permita acesso SSH e verifique se a instância tem conectividade com a Internet. Você fornece o arquivo `.pem` para o par de chaves quando se conecta à instância.

Use o procedimento a seguir para se conectar à instância MAC usando um cliente SSH. Se você receber um erro ao tentar se conectar à instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#).

### Para se conectar à sua instância usando SSH

1. Verifique se o computador local tem um cliente SSH instalado digitando `ssh` na linha de comando. Se o computador não reconhecer o comando, procure um cliente SSH para seu sistema operacional e instale-o.
2. Obtenha o nome público do DNS da sua instância. Usando o console da Amazon EC2, você pode encontrar o nome público do DNS nas guias **Details** (Detalhes) e **Networking (Rede)**. Usando o AWS CLI, você pode encontrar o nome público do DNS usando o comando [describe-instances](#).
3. Localize o arquivo `.pem` do par de chaves que você especificou quando executou a instância.
4. Conecte-se à instância usando o comando `ssh`, especificando o nome público do DNS da instância e do arquivo `.pem`.

```
ssh -i /path/my-key-pair.pem ec2-user@my-instance-public-dns-name
```

## Conecte-se à instância usando o Apple Remote Desktop

Use o procedimento a seguir para se conectar à instância usando o Apple Remote Desktop (ARD).

Para se conectar à instância usando o ARD

1. Verifique se o computador local tem um cliente ARD ou um cliente VNC que suporte uma instalação do ARD. No macOS, você pode usar a aplicação de compartilhamento de tela integrado. Caso contrário, procure um cliente VNC para o sistema operacional e instale-o.
2. No computador local, [conecte-se à instância usando SSH \(p. 267\)](#).
3. Defina uma senha para a conta ec2-user usando o comando passwd da seguinte forma.

```
[ec2-user ~]$ sudo passwd ec2-user
```

4. Inicie o agente do Apple Remote Desktop e ative o acesso ao desktop remoto da seguinte forma.

```
[ec2-user ~]$ sudo /System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart \
-activate -configure -access -on \
-restart -agent -privs -all
```

5. No computador, conecte-se à instância usando o comando ssh. Além das opções mostradas na seção anterior, use a opção -L para habilitar o encaminhamento de porta e encaminhar todo o tráfego na porta local 5900 para o servidor ARD na instância.

```
ssh -L 5900:localhost:5900 -i /path/my-key-pair.pem ec2-user@my-instance-public-dns-name
```

6. No computador local, use o cliente ARD, ou o cliente VNC que suporta ARD, para se conectar ao localhost na porta 5900. Por exemplo, use a aplicação de compartilhamento de tela no macOS da seguinte forma:
  - a. Abra o Finder e inicie a aplicação de compartilhamento de tela.
  - b. Em Connect to (Conectar-se a), digite **localhost**.
  - c. Faça login conforme solicitado, usando **ec2-user** como nome de usuário e a senha que você criou para a conta ec2-user.

## Modificar a resolução de tela do macOS em instâncias Mac

Depois de se conectar à instância Mac do EC2 usando ARD ou um cliente VNC compatível com ARD instalado, você pode modificar a resolução de tela do seu ambiente macOS usando qualquer uma das ferramentas ou utilitários macOS disponíveis publicamente, como [displayplacer](#)

Modificar a resolução da tela usando o displayplacer

1. Instale o displayplacer.

```
brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Mostre as informações atuais da tela e possíveis resoluções de tela.

```
displayplacer list
```

3. Aplique a resolução de tela desejada.

```
displayplacer "id:<screenID> res:<width>x<height> origin:(0,0) degree:0"
```

Por exemplo:

```
RES="2560x1600"  
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off origin:  
(0,0) degree:0"
```

## AMIs do macOS do EC2

O macOS Amazon EC2 foi projetado para fornecer um ambiente estável, seguro e de alta performance para workloads de desenvolvedores executadas em instâncias Mac do Amazon EC2. As AMIs do macOS do EC2 também incluem vários pacotes que permitem a fácil integração com o AWS, incluindo ferramentas de configuração de execução bibliotecas e ferramentas populares do AWS . Por padrão, as AMIs do macOS do EC2 incluem:

- Drivers do ENA
- EC2 MacOS Init
- Monitoramento do EC2 System para macOS
- SSM Agent para macOS
- AWS Command Line Interface (AWS CLI) versão 2
- Ferramentas de linha de comando para Xcode
- Homebrew

O AWS fornece AMIs do macOS do EC2 atualizadas regularmente que incluem atualizações para pacotes de propriedade da AWS e a versão mais recente do macOS totalmente testada. Além disso, o AWS fornece AMIs atualizadas com as atualizações mais recentes da versão secundária ou da versão principal assim que elas puderem ser totalmente testadas e aprovadas. Se você não precisar preservar dados ou personalizações das instâncias Mac, poderá obter as atualizações mais recentes ao executar uma nova instância usando a AMI atual e encerrando a instância anterior. Caso contrário, você pode escolher quais atualizações se aplicam às instâncias Mac.

## Atualizar o sistema operacional e o software

Você pode instalar atualizações do sistema operacional da Apple usando o comando softwareupdate.

Para instalar atualizações do sistema operacional da Apple

1. Liste os pacotes com atualizações disponíveis usando o seguinte comando.

```
[ec2-user ~]$ softwareupdate --list
```

2. Instale todas as atualizações ou apenas atualizações específicas. Para instalar atualizações específicas, use o seguinte comando.

```
[ec2-user ~]$ sudo softwareupdate --install label
```

Para instalar todas as atualizações, use o seguinte comando.

```
[ec2-user ~]$ sudo softwareupdate --install --all
```

Os administradores de sistemas podem usar AWS Systems Manager para implementar atualizações pré-aprovadas do sistema operacional. Para obter mais informações, consulte o [Guia do usuário do AWS Systems Manager](#).

Você pode usar o Homebrew para instalar atualizações de pacotes nas AMIs do macOS do EC2, para ter a versão mais recente destes pacotes nas suas instâncias. Você também pode usar o Homebrew para instalar e executar aplicações macOS comuns no macOS do Amazon EC2. Para obter mais informações, consulte a [Documentação do Homebrew](#).

Para instalar atualizações usando o Homebrew

1. Atualize o Homebrew usando o seguinte comando.

```
[ec2-user ~]$ brew update
```

2. Liste os pacotes com atualizações disponíveis usando o seguinte comando.

```
[ec2-user ~]$ brew outdated
```

3. Instale todas as atualizações ou apenas atualizações específicas. Para instalar atualizações específicas, use o seguinte comando.

```
[ec2-user ~]$ brew upgrade formula
```

Para instalar todas as atualizações, use o seguinte comando.

```
[ec2-user ~]$ brew upgrade
```

#### Warning

Não instale versões beta ou pré-lançamento do macOS em suas instâncias do EC2 Mac, pois essa configuração não é compatível no momento. A instalação de versões beta ou pré-lançamento do macOS levará à degradação do Host Dedicado do EC2 Mac quando você interromper ou encerrar sua instância e impedirá que você inicie ou abra uma nova instância nesse host.

## EC2 MacOS Init

O EC2 macOS Init é usado para inicializar instâncias Mac do EC2 na inicialização. Ele usa grupos prioritários para executar grupos lógicos de tarefas ao mesmo tempo.

O arquivo plist launchd é `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. Os arquivos do EC2 macOS Init estão localizados no `/usr/local/aws/ec2-macos-init`.

Para obter mais informações, consulte <https://github.com/aws/ec2-macos-init>.

## Monitoramento do EC2 System para macOS

O Monitoramento do EC2 System para macOS fornece métricas de utilização da CPU para Amazon CloudWatch. Ele envia essas métricas para o CloudWatch por meio de um dispositivo serial personalizado em períodos de 1 minuto. Você pode ativar ou desativar este agente da seguinte forma. Ele é habilitado por padrão.

```
sudo setup-ec2monitoring [enable | disable]
```

## Aumente o tamanho de um volume do EBS na instância do Mac

Você pode aumentar o tamanho dos volumes do Amazon EBS na sua instância do Mac. Para obter mais informações, consulte [Volumes elásticos do Amazon EBS \(p. 1405\)](#).

Depois de aumentar o tamanho do volume, você deve aumentar o tamanho do contêiner APFS da forma a seguir.

Disponibilizar maior espaço em disco para uso

1. Determine se uma reinicialização é necessária. Se você redimensionou um volume do EBS existente em uma instância Mac em execução, será necessário [reiniciar](#) a instância para disponibilizar o novo tamanho. Se a modificação do espaço em disco tiver sido feita durante o tempo de inicialização, não será necessária uma reinicialização.

Exibir o status atual dos tamanhos de disco:

```
[ec2-user ~]$ diskutil list external physical
/dev/disk0 (external, physical):
#:          TYPE NAME                SIZE    IDENTIFIER
0: GUID_partition_scheme          *322.1 GB   disk0
1:           EFI #EFI#              209.7 MB   disk0s1
2:           Apple_APFS #Container disk2#      321.9 GB   disk0s2
```

2. Copie e cole o seguinte comando.

```
PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -d" "
-f8)
yes | sudo diskutil repairDisk $PDISK
```

3. Copie e cole o seguinte comando.

```
sudo diskutil apfs resizeContainer $APFSCONT 0
```

## Interromper e encerrar a instância do Mac

Quando você interrompe uma instância do Mac, ela permanece no estado `stopping` por cerca de 15 minutos antes de entrar no estado `stopped`.

Quando você interrompe ou encerra uma instância do Mac, o Amazon EC2 executa um fluxo de trabalho de depuração no Host dedicado subjacente para apagar o SSD interno, para limpar as variáveis NVRAM persistentes e, se necessário, para atualizar o software bridgeOS no Mac mini subjacente. Isso garante que as instâncias Mac fornecem a mesma segurança e privacidade de dados que outras instâncias do EC2 Nitro. Isso também permite que você execute as AMIs mais recentes do macOS sem atualizar manualmente o software bridgeOS. Durante o fluxo de trabalho de depuração, o Host dedicado entra temporariamente no estado `pending`. Se o software bridgeOS não precisar ser atualizado, o fluxo de trabalho de depuração demora até 50 minutos para ser concluído. Se o software bridgeOS precisar ser atualizado, o fluxo de trabalho de depuração pode levar até 3 horas para ser concluído.

Não é possível iniciar a instância do Mac interrompida ou iniciar uma nova instância do Mac até que o fluxo de trabalho de depuração seja concluído, momento no qual o estado Host dedicado entra no estado `available`.

A medição e o faturamento são pausados quando o host dedicado entra no estado `pending`. Você não será cobrado pela duração do fluxo de trabalho de depuração.

## Assinar notificações de AMI do macOS

Para ser notificado sobre o lançamento de novas AMIs ou atualizações do bridgeOS, inscreva-se em notificações usando o Amazon SNS.

Para assinar notificações de AMI do macOS

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-1:898855652048:amazon-ec2-macos-ami-updates**
    - **arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates**

Em Protocol (Protocolo):

- b. E-mail:

Para Endpoint, digite um endereço de e-mail que você pode usar para receber as notificações. Após criar a assinatura, você receberá uma mensagem de confirmação com a linha de assunto **AWS Notification - Subscription Confirmation**. Abra o e-mail e escolha Confirm subscription para concluir a assinatura.

- c. SMS:

Em Endpoint, digite um número de telefone que você pode usar para receber as notificações.

- d. AWS Lambda, Amazon SQS, Amazon Kinesis Data Firehose (As notificações virão no formato JSON):

Em Endpoint, insira o ARN da função Lambda, fila SQS ou transmissão do Firehose que você pode usar para receber notificações.

- e. Selecione Create subscription.

Sempre que AMIs do macOS forem lançadas, enviaremos notificações aos assinantes do tópico **amazon-ec2-macos-ami-updates**. Sempre que houver uma atualização do bridgeOS, enviaremos notificações aos assinantes do tópico **amazon-ec2-bridgeos-updates**. 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 macOS

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 criadas 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.

## Libere o Host dedicado para a sua instância do Mac

Quando você terminar de usar a instância Mac, poderá liberar o Host dedicado. Antes de liberar o Host dedicado, você deve interromper ou encerrar a instância Mac. Você não pode liberar o host até que o período de alocação exceda o mínimo de 24 horas.

### Para liberar o Host dedicado

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 Instance state (Estado da instância) e, em seguida, escolha Stop instance (Interromper instância) ou Terminate instance (Encerrar instância).
4. No painel de navegação, selecione Hosts dedicados.
5. Selecione o Host dedicado e escolha Actions (Ações), Release host (Liberar host).
6. Quando for solicitada a confirmação, escolha Release (Liberar).

## 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.meta1, 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](#).

### Instâncias C6g, C6gd e C6gn

Essas instâncias são habilitadas pelos processadores AWS Graviton2 e são ideais para executar workloads avançadas de uso intensivo de computação, como as seguintes:

- High-Performance Computing (HPC – Computação de alta performance)
- Processamento em lotes
- Veiculação de anúncios
- Codificação de vídeo
- Servidores de jogos
- Modelagem científica
- Análise distribuída
- Inferência de machine learning baseada em CPU

As instâncias bare metal, como a `c6g.metal`, fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória.

Para obter mais informações, consulte [Instâncias C6g do Amazon EC2](#).

#### Tópicos

- [Especificações de hardware \(p. 274\)](#)
- [Da performance da instância \(p. 276\)](#)
- [Performance das redes \(p. 277\)](#)
- [Performance de E/S em SSD \(p. 279\)](#)
- [Recursos da instância \(p. 280\)](#)
- [Notas de release \(p. 281\)](#)

## 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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Otimizadas para computação

---

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
c6g.medium	1	2
c6g.large	2	4
c6g.xlarge	4	8
c6g.2xlarge	8	16
c6g.4xlarge	16	32

Tipo de instância	vCPUs padrão	Memória (GiB)
c6g.8xlarge	32	64
c6g.12xlarge	48	96
c6g.16xlarge	64	128
c6g.metal	64	128
c6gd.medium	1	2
c6gd.large	2	4
c6gd.xlarge	4	8
c6gd.2xlarge	8	16
c6gd.4xlarge	16	32
c6gd.8xlarge	32	64
c6gd.12xlarge	48	96
c6gd.16xlarge	64	128
c6gd.metal	64	128
c6gn.medium	1	2
c6gn.large	2	4
c6gn.xlarge	4	8
c6gn.2xlarge	8	16
c6gn.4xlarge	16	32
c6gn.8xlarge	32	64
c6gn.12xlarge	48	96
c6gn.16xlarge	64	128

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. 616).

## 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. 1438).

Alguns tipos de instância otimizados para computação fornecem a capacidade de controlar C-states e P-states do processador no Linux. Os C-states controlam os níveis de suspensão em que um núcleo pode entrar quando estiver inativo, enquanto os P-states controlam a performance desejada (em frequência

da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para a instância do EC2 \(p. 604\)](#).

## 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 Linux \(p. 1015\)](#).

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	<a href="#">Intel 82599 VF (p. 1026)</a>
c4.xlarge   c4.2xlarge   c4.4xlarge	Alto	<a href="#">Intel 82599 VF (p. 1026)</a>
c5.4xlarge e menor   c5a.4xlarge e menor   c5ad.4xlarge e menor   c5d.4xlarge e menor   c6g.4xlarge e menor   c6gd.4xlarge e menor	Até 10 Gbps †	<a href="#">ENA (p. 1016)</a>
c4.8xlarge	10 Gbps	<a href="#">Intel 82599 VF (p. 1026)</a>
c5.9xlarge   c5a.8xlarge   c5ad.8xlarge   c5d.9xlarge	10 Gbps	<a href="#">ENA (p. 1016)</a>
c5.12xlarge   c5a.12xlarge   c5ad.12xlarge   c5d.12xlarge   c6g.8xlarge   c6gd.8xlarge	12 Gbps	<a href="#">ENA (p. 1016)</a>
c5a.16xlarge   c5a.24xlarge   c5ad.16xlarge   c5ad.24xlarge   c6g.12xlarge   c6gd.12xlarge	20 Gbps	<a href="#">ENA (p. 1016)</a>
c5n.4xlarge e menor   c6gn.4xlarge e menor	Até 25 Gbps †	<a href="#">ENA (p. 1016)</a>
c5.18xlarge   c5.24xlarge   c5.metal   c5d.18xlarge   c5d.24xlarge   c5d.metal   c6g.16xlarge   c6g.metal   c6gd.16xlarge   c6gd.metal   c6gn.4xlarge	25 Gbps	<a href="#">ENA (p. 1016)</a>
c5n.9xlarge   c6gn.8xlarge	50 Gbps	<a href="#">ENA (p. 1016)</a>
c6gn.12xlarge	75 Gbps	<a href="#">ENA (p. 1016)</a>
c5n.18xlarge   c5n.metal   c6gn.16xlarge	100 Gbps	<a href="#">ENA (p. 1016), EFA (p. 1044)</a>

† 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 \(p. 1013\)](#).

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
c5.large	.75	10
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
c6g.medium	5.	10
c6g.large	.75	10
c6g.xlarge	1.25	10
c6g.2xlarge	2,5	10
c6g.4xlarge	5	10
c6gd.medium	5.	10
c6gd.large	.75	10
c6gd.xlarge	1.25	10
c6gd.2xlarge	2,5	10
c6gd.4xlarge	5	10

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
c6gn.medium	1.6	25
c6gn.large	3	25
c6gn.xlarge	6.3	25
c6gn.2xlarge	12,5	25
c6gn.4xlarge	15	25

## Performance de E/S em SSD

Se você usar a AMI do Linux com kernel versão 4.4 ou superior e 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
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
c6gd.medium	13.438	5.625
c6gd.large	26.875	11.250

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
c6gd.xlarge	53.750	22.500
c6gd.2xlarge	107.500	45.000
c6gd.4xlarge	215.000	90.000
c6gd.8xlarge	430.000	180.000
c6gd.12xlarge	645.000	270.000
c6gd.16xlarge	860.000	360.000
c6gd.metal	860.000	360.000

\* 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 \(p. 1510\)](#).

## 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

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
C5ad	Não	Sim	NVMe *	Sim
C5d	Não	Sim	NVMe *	Sim
C5n	Sim	Sim	Não	Sim
C6g	Sim	Sim	Não	Sim
C6gd	Não	Sim	NVMe *	Sim
C6gn	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 Linux \(p. 1434\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1494\)](#)
- [Grupos de posicionamento \(p. 1084\)](#)

## 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 C6g, C6gd e C6gn tem um processador AWS Graviton2 baseado na arquitetura Arm de 64 bits.
- As instâncias C4 e instâncias baseadas no [sistema Nitro \(p. 210\)](#) 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 \(p. 1434\)](#) devem estar instalados
  - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1016\)](#) devem estar instalados

As AMIs do Linux a seguir atendem a esses requisitos:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (com kernel linux-aws) ou posterior
- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior
- As instâncias com processadores AWS Graviton têm os seguintes requisitos:
  - Use uma AMI para a arquitetura Arm de 64 bits.

- Suporte à inicialização por meio de UEFI com tabelas de ACPI e oferecer suporte a hot-plug ACPI ou a dispositivos PCI.

As AMIs a seguir atendem a esses requisitos:

- Amazon Linux 2 (Arm de 64 bits)
- Ubuntu 16.04 ou posterior (Arm de 64 bits)
- Red Hat Enterprise Linux 8.0 ou posterior (Arm de 64 bits)
- SUSE Linux Enterprise Server 15 ou posterior (Arm de 64 bits)
- Debian 10 ou posterior (Arm de 64 bits)
- 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 \(p. 1520\)](#).
- Para obter a melhor performance de suas instâncias C6gn, certifique-se de que elas tenham o driver ENA versão 2.2.9 ou posterior. Usar um driver ENA anterior à versão 1.2 com essas instâncias causará falhas no anexo da interface de rede. As AMIs a seguir têm driver ENA compatível.
  - Amazon Linux 2 com kernel 4.14.186
  - Ubuntu 20.04 com kernel 5.4.0-1025-aws
  - Red Hat Enterprise Linux 8.3 com kernel 4.18.0-240.1.1.el8\_3.arch
  - SUSE Linux Enterprise Server 15 SP2 com kernel 5.3.18-24.15.1
- [Oespelhamento de tráfego](#) não é suportado em instâncias C6gn.
- Para executar AMIs para todas as distribuições Linux em instâncias C6gn, use AMIs com a versão mais recente e execute uma atualização para o driver mais recente. Para versões anteriores, baixe o driver mais recente do [GitHub](#).
- 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. O Amazon Linux 2 e as versões mais recentes da AMI do Amazon Linux são compatíveis com PCIe hotplug nativo, mas as versões anteriores não são. Você precisa ativar as seguintes opções de configuração do kernel do Linux:

```
CONFIG_HOTPLUG_PCI_PCIE=y  
CONFIG_PCIEASPM=y
```

- 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 criadas no sistema Nitro devem ter acpid instalado para oferecer suporte ao desligamento normal por meio de solicitações de API.
- 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 R6g e R6gd

Essas instâncias são desenvolvidas por processadores AWS Graviton2 e são ideais para executar workloads com uso intensivo de memória, como as seguintes:

- Bancos de dados de código aberto (por exemplo, MySQL, MariaDB e PostgreSQL)
- Caches de memória (por exemplo, Memcached, Redis e KeyDB)

As instâncias bare metal, como a `r6g.meta1`, fornecem aos aplicativos acesso direto aos recursos físicos do servidor host, como processadores e memória.

Para obter mais informações, consulte [Instâncias R6g 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 X2gd

Essas instâncias são ideais para o seguinte:

- Bancos de dados em memória, como Redis e Memcached.
- Bancos de dados relacionais, como MySQL e PostgreSQL.
- Workloads Electronic Design Automation (EDA), como verificação física e ferramentas de layout.
- Workloads com uso intensivo de memória, como análises em tempo real e servidores de cache em tempo real.

Para obter mais informações, consulte [Instâncias X2gd 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.meta1` 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 \(p. 284\)](#)
- [Performance da memória \(p. 288\)](#)
- [Performance da instância \(p. 289\)](#)
- [Performance das redes \(p. 289\)](#)
- [Performance de E/S em SSD \(p. 292\)](#)
- [Recursos da instância \(p. 294\)](#)
- [Suporte para vCPUs \(p. 295\)](#)
- [Notas de release \(p. 296\)](#)

## Especificações de hardware

Este é um resumo das especificações de hardware para instâncias otimizadas para memória.

Tipo de instância	vCPUs padrão	Memória (GiB)
r4.large	2	15.25
r4.xlarge	4	30.5
r4.2xlarge	8	61
r4.4xlarge	16	122
r4.8xlarge	32	244
r4.16xlarge	64	488
r5.large	2	16
r5.xlarge	4	32
r5.2xlarge	8	64
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

Tipo de instância	vCPUs padrão	Memória (GiB)
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
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

Tipo de instância	vCPUs padrão	Memória (GiB)
r5n.8xlarge	32	256
r5n.12xlarge	48	384
r5n.16xlarge	64	512
r5n.24xlarge	96	768
r5n.metal	96	768
r6g.medium	1	8
r6g.large	2	16
r6g.xlarge	4	32
r6g.2xlarge	8	64
r6g.4xlarge	16	128
r6g.8xlarge	32	256
r6g.12xlarge	48	384
r6g.16xlarge	64	512
r6gd.medium	1	8
r6gd.large	2	16
r6gd.xlarge	4	32
r6gd.2xlarge	8	64
r6gd.4xlarge	16	128
r6gd.8xlarge	32	256
r6gd.12xlarge	48	384
r6gd.16xlarge	64	512
u-6tb1.56xlarge	224	6,144
u-6tb1.112xlarge	448	6,144
u-6tb1.metal	448 *	6,144
u-9tb1.112xlarge	448	9,216
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

Tipo de instância	vCPUs padrão	Memória (GiB)
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
x2gd.medium	1	16
x2gd.large	2	32
x2gd.xlarge	4	64
x2gd.2xlarge	8	128
x2gd.4xlarge	16	256
x2gd.8xlarge	32	512
x2gd.12xlarge	48	768
x2gd.16xlarge	64	1,024
x2gd.metal	64	1,024
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. 616).

## 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 \(p. 284\)](#).

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. Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#).

## 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.

Algumas instâncias otimizadas na memória fornecem a capacidade de controlar C-states e P-states do processador no Linux. Os C-states controlam os níveis de suspensão nos quais um núcleo pode entrar quando está inativo, enquanto os P-states controlam a performance desejada (medido pela frequência da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para a instância do EC2 \(p. 604\)](#).

## 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 Linux \(p. 1015\)](#).

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   r6g.4xlarge e menor   r6gd.4xlarge e menor   x1e.8large e menor   x2gd.4xlarge e menor   z1d.3xlarge e menor	Até 10 Gbps †	<a href="#">ENA (p. 1016)</a>
r4.8xlarge   r5.8xlarge   r5.12xlarge   r5a.12xlarge   r5ad.12xlarge   r5b.8xlarge   r5b.12xlarge   r5d.8xlarge   r5d.12xlarge   x1.16xlarge   xle.16xlarge   z1d.6xlarge	10 Gbps	<a href="#">ENA (p. 1016)</a>
r5a.16xlarge   r5ad.16xlarge   r6g.8xlarge   r6gd.8xlarge   x2gd.8xlarge	12 Gbps	<a href="#">ENA (p. 1016)</a>
r5.16xlarge   r5a.24xlarge   r5ad.24xlarge   r5b.16xlarge   r5d.16xlarge   r6g.12xlarge   r6gd.12xlarge   x2gd.12xlarge	20 Gbps	<a href="#">ENA (p. 1016)</a>
r5dn.4xlarge e menor   r5n.4xlarge e menor	Até 25 Gbps †	<a href="#">ENA (p. 1016)</a>

Tipo de instância	Performance das redes	Redes avançadas
r4.16xlarge   r5.24xlarge   r5.metal   r5b.24xlarge   r5b.metal   r5d.24xlarge   r5d.metal   r5dn.8xlarge   r5n.8xlarge   r6g.16xlarge   r6g.metal   r6gd.16xlarge   r6gd.metal   x1.32xlarge   x1e.32xlarge   x2gd.16xlarge   x2gd.metal   z1d.12xlarge   z1d.metal	25 Gbps	<a href="#">ENA (p. 1016)</a>
r5dn.12xlarge   r5n.12xlarge	50 Gbps	<a href="#">ENA (p. 1016)</a>
r5dn.16xlarge   r5n.16xlarge	75 Gbps	<a href="#">ENA (p. 1016)</a>
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	<a href="#">ENA (p. 1016)</a>

\* 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 \(p. 1013\)](#).

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

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
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
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
r6g.medium	5.	10
r6g.large	.75	10
r6g.xlarge	1.25	10
r6g.2xlarge	2,5	10
r6g.4xlarge	5	10
r6gd.medium	5.	10
r6gd.large	.75	10
r6gd.xlarge	1.25	10
r6gd.2xlarge	2,5	10
r6gd.4xlarge	5	10
x2gd.medium	5.	10
x2gd.large	.75	10
x2gd.xlarge	1.25	10

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
<b>x2gd.2xlarge</b>	2,5	10
<b>x2gd.4xlarge</b>	5	10
<b>z1d.large</b>	.75	10
<b>z1d.xlarge</b>	1.25	10
<b>z1d.2xlarge</b>	2,5	10
<b>z1d.3xlarge</b>	5	10

## Performance de E/S em SSD

Se você usar a AMI do Linux com kernel versão 4.4 ou superior e 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
<b>r5ad.large *</b>	30.000	15.000
<b>r5ad.xlarge *</b>	59.000	29.000
<b>r5ad.2xlarge *</b>	117.000	57.000
<b>r5ad.4xlarge *</b>	234.000	114.000
<b>r5ad.8xlarge</b>	466.666	233.333
<b>r5ad.12xlarge</b>	700.000	340.000
<b>r5ad.16xlarge</b>	933.333	466.666
<b>r5ad.24xlarge</b>	1.400.000	680.000
<b>r5d.large *</b>	30.000	15.000
<b>r5d.xlarge *</b>	59.000	29.000
<b>r5d.2xlarge *</b>	117.000	57.000
<b>r5d.4xlarge *</b>	234.000	114.000
<b>r5d.8xlarge</b>	466.666	233.333
<b>r5d.12xlarge</b>	700.000	340.000
<b>r5d.16xlarge</b>	933.333	466.666
<b>r5d.24xlarge</b>	1.400.000	680.000
<b>r5d.metal</b>	1.400.000	680.000
<b>r5dn.large *</b>	30.000	15.000

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
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
r6gd.medium	13.438	5.625
r6gd.large	26.875	11.250
r6gd.xlarge	53.750	22.500
r6gd.2xlarge	107.500	45.000
r6gd.4xlarge	215.000	90.000
r6gd.8xlarge	430.000	180.000
r6gd.12xlarge	645.000	270.000
r6gd.16xlarge	860.000	360.000
r6gd.metal	860.000	360.000
x2gd.medium	13.438	5.625
x2gd.large	26.875	11.250
x2gd.xlarge	53.750	22.500
x2gd.2xlarge	107.500	45.000
x2gd.4xlarge	215.000	90.000
x2gd.8xlarge	430.000	180.000
x2gd.12xlarge	645.000	270.000
x2gd.16xlarge	860.000	360.000
x2gd.metal	860.000	360.000
z1d.large *	30.000	15.000
z1d.xlarge *	59.000	29.000
z1d.2xlarge *	117.000	57.000
z1d.3xlarge *	175.000	75.000

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
<b>z1d.6xlarge</b>	350,000	170,000
<b>z1d.12xlarge</b>	700,000	340,000
<b>z1d.metal</b>	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 \(p. 1510\)](#).

## 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

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
R5n	Sim	Sim	Não	Sim
R6g	Sim	Sim	Não	Sim
R6gd	Não	Sim	NVMe *	Sim
Mais memória	Sim	Sim	Não	Virtualizada: sim Bare metal: não
X1	Não	Não	SSD	Sim
X2gd	Não	Sim	NVME *	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 Linux \(p. 1434\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1494\)](#)
- [Grupos de posicionamento \(p. 1084\)](#)

## Suporte 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.
- O recurso de instâncias R6g e R6gd têm um processador AWS Graviton2 baseado na arquitetura Arm de 64 bits.
- 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 \(p. 1434\)](#) devem estar instalados
  - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1016\)](#) devem estar instalados

As AMIs do Linux a seguir atendem a esses requisitos:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (com kernel `linux-aws`) ou posterior
- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior
- As instâncias com processadores AWS Graviton têm os seguintes requisitos:
  - Use uma AMI para a arquitetura Arm de 64 bits.
  - Suporte à inicialização por meio de UEFI com tabelas de ACPI e oferecer suporte a hot-plug ACPI ou a dispositivos PCI.

As AMIs a seguir atendem a esses requisitos:

- Amazon Linux 2 (Arm de 64 bits)
- Ubuntu 16.04 ou posterior (Arm de 64 bits)
- Red Hat Enterprise Linux 8.0 ou posterior (Arm de 64 bits)
- SUSE Linux Enterprise Server 15 ou posterior (Arm de 64 bits)
- Debian 10 ou posterior (Arm de 64 bits)
- 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 \(p. 1520\)](#).
- 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. O Amazon Linux 2 e as versões mais recentes da AMI do Amazon Linux são compatíveis com PCIe hotplug nativo, mas as versões anteriores não são. Você precisa ativar as seguintes opções de configuração do kernel do Linux:

```
CONFIG_HOTPLUG_PCI_PCIE=y  
CONFIG_PCIEASPM=y
```

- 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 `r4.1.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 \(p. 298\)](#)
- [Da performance da instância \(p. 300\)](#)
- [Performance das redes \(p. 300\)](#)
- [Performance de E/S em SSD \(p. 301\)](#)
- [Recursos da instância \(p. 303\)](#)
- [Suporte para vCPUs \(p. 303\)](#)
- [Notas de release \(p. 304\)](#)

## 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 \(p. 1494\)](#) e [Volumes de armazenamento de instâncias SSD \(p. 1508\)](#).

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. 616).

## Da performance da instância

Para garantir a melhor performance de taxa de transferência do disco de sua instância no Linux, recomendamos que você use a versão mais recente do Amazon Linux 2 ou do Amazon Linux AMI.

Para instâncias com volumes de armazenamento de instâncias NVMe, você deve usar uma AMI do Linux com kernel versão 4.4 ou superior. Caso contrário, sua instância não conseguirá a performance máxima de IOPS disponível.

As instâncias D2 oferecem a melhor performance do disco quando você usa um kernel Linux que ofereça suporte a concessões persistentes, uma extensão para o protocolo de anel de bloco Xen que melhora significativamente a escalabilidade e a taxa de transferência do disco. Para obter mais informações sobre as concessões persistentes, consulte [este artigo](#) no Blog do projeto Xen.

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. 1438).

Alguns tipos de instância otimizados para armazenamento fornecem a capacidade de controlar C-states e P-states do processador no Linux. Os C-states controlam os níveis de suspensão em que um núcleo pode entrar quando estiver inativo, enquanto os P-states controlam a performance desejada (em frequência da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para a instância do EC2](#) (p. 604).

## 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 Linux](#) (p. 1015).

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	<a href="#">Intel 82599 VF</a> (p. 1026)
d2.2xlarge   d2.4xlarge	Alto	<a href="#">Intel 82599 VF</a> (p. 1026)
i3.4xlarge e menor	Até 10 Gbps †	<a href="#">ENA</a> (p. 1016)
d2.8xlarge	10 Gbps	<a href="#">Intel 82599 VF</a> (p. 1026)
i3.8xlarge   h1.8xlarge	10 Gbps	<a href="#">ENA</a> (p. 1016)
d3.4xlarge e menor	Até 15 Gbps †	<a href="#">ENA</a> (p. 1016)
d3en.2xlarge e menor   i3en.3xlarge e menor	Até 25 Gbps †	<a href="#">ENA</a> (p. 1016)

Tipo de instância	Performance das redes	Redes avançadas
d3.8xlarge   d3en.4xlarge   i3.16xlarge   i3.metal   i3en.6xlarge   h1.16xlarge	25 Gbps	<a href="#">ENA (p. 1016)</a>
d3en.6xlarge	40 Gbps	<a href="#">ENA (p. 1016)</a>
d3.8xlarge   d3en.8xlarge   i3en.12xlarge	50 Gbps	<a href="#">ENA (p. 1016)</a>
d3en.12xlarge	75 Gbps	<a href="#">ENA (p. 1016)</a>
i3en.24xlarge   i3en.metal	100 Gbps	<a href="#">ENA (p. 1016), EFA (p. 1044)</a>

† 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 \(p. 1013\)](#).

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 usar a AMI do Linux com kernel versão 4.4 ou superior e 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

Tamanho de instância	100% de IOPS de leitura aleatória	IOPS de gravação
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
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 \(p. 1510\)](#).

## 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 Linux \(p. 1434\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1494\)](#)
- [Grupos de posicionamento \(p. 1084\)](#)

## Suporte para vCPUs

O tipo de instância d2.8xlarge fornece 36 vCPUs, que podem causar problemas de inicialização em alguns sistemas operacionais Linux que têm um limite de 32 vCPU. Recomendamos enfaticamente que você use as AMIs mais recentes ao executar as instâncias d2.8xlarge.

As AMIs do Linux a seguir oferecem suporte à execução das instâncias d2.8xlarge com 36 vCPUs:

- [Amazon Linux 2 \(HVM\)](#)
- [AMI do Amazon Linux 2018.03 \(HVM\)](#)
- [Ubuntu Server 14.04 LTS \(HVM\) ou posterior](#)
- [Red Hat Enterprise Linux 7.1 \(HVM\)](#)
- [SUSE Linux Enterprise Server 12 \(HVM\)](#)

Se você precisar usar AMIs diferentes para sua aplicação e a execução da sua instância d2.8xlarge não for concluída com êxito (por exemplo, se o status da instância mudar para `stopped` durante a inicialização com o motivo de transição de estado para `Client.InstanceInitiatedShutdown`), modifique sua instância como descrito no procedimento a seguir para oferecer suporte a mais de 32 vCPUs, de modo que você possa usar o tipo de instância d2.8xlarge.

Para atualizar uma instância para oferecer suporte a mais de 32 vCPUs

1. Execute uma instância D2 usando sua AMI, escolhendo qualquer tipo de instância D2 além de d2.8xlarge.
2. Atualize o kernel para a versão mais recente seguindo as instruções específicas do sistema operacional. Por exemplo, para RHEL 6, use o comando a seguir:

```
sudo yum update -y kernel
```

3. Pare a instância.
4. (Opcional) Crie uma AMI a partir da instância que você pode usar para executar todas as instâncias d2.8xlarge adicionais de que precisar no futuro.
5. Altere o tipo da sua instância parada para d2.8xlarge (selecione Actions (Ações), Instance settings (Configurações da instância), Change instance type (Alterar tipo de instância) e siga as instruções).
6. Inicie a instância. Se a instância for executada corretamente, pronto. Se a instância ainda não inicializar corretamente, vá para a próxima etapa.
7. (Opcional) Se a instância ainda não inicializar corretamente, o kernel na sua instância pode não suportar mais de 32 vCPUs. Contudo, você pode conseguir inicializar a instância se limitar as vCPUs.
  - a. Altere o tipo da sua instância interrompida para qualquer tipo de instância D2 diferente de d2.8xlarge (selecione Actions (Ações), Instance settings (Configurações da instância), Change instance type (Alterar tipo de instância) e siga as instruções).
  - b. Adicione a opção `maxcpus=32` ao seus parâmetros de kernel de inicialização seguindo as instruções específicas do sistema operacional. Por exemplo, para RHEL 6, edite o arquivo `/boot/grub/menu.lst` e adicione a opção a seguir à entrada `kernel` mais recente e ativa:

```
default=0
timeout=1
splashimage=(hd0,0)/boot/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux Server (2.6.32-504.3.3.el6.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-2.6.32-504.3.3.el6.x86_64 maxcpus=32 console=ttyS0 ro
root=UUID=9996863e-b964-47d3-a33b-3920974fdbd9 rd_NO_LUKS KEYBOARDTYPE=pc
KEYTABLE=us LANG=en_US.UTF-8 xen_blkfront.sda_is_xvda=1 console=ttyS0,115200n8
console=tty0 rd_NO_MD SYSFONT=latarcyrheb-sun16 crashkernel=auto rd_NO_LVM
rd_NO_DM
initrd /boot/initramfs-2.6.32-504.3.3.el6.x86_64.img
```

- c. Pare a instância.
- d. (Opcional) Crie uma AMI a partir da instância que você pode usar para executar todas as instâncias d2.8xlarge adicionais de que precisar no futuro.
- e. Altere o tipo da sua instância parada para d2.8xlarge (selecione Actions (Ações), Instance settings (Configurações da instância), Change instance type (Alterar tipo de instância) e siga as instruções).
- f. Inicie a instância.

## Notas de release

- Você deve executar instâncias otimizadas de armazenamento usando uma AMI HVM. Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#).
- As instâncias criadas no [Sistema Nitro \(p. 210\)](#) têm os seguintes requisitos:
  - Os [drivers de NVMe \(p. 1434\)](#) devem estar instalados
  - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1016\)](#) devem estar instalados

As AMIs do Linux a seguir atendem a esses requisitos:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (com kernel `linux-aws`) ou posterior
- Red Hat Enterprise Linux 7.4 ou posterior

- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior
- 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. O Amazon Linux 2 e as versões mais recentes da AMI do Amazon Linux são compatíveis com PCIe hotplug nativo, mas as versões anteriores não são. Você precisa ativar as seguintes opções de configuração do kernel do Linux:

```
CONFIG_HOTPLUG_PCI_PCIE=y  
CONFIG_PCIEASPM=y
```

- 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.
- Com as FreeBSD AMIs, as instâncias bare metal demoram quase uma hora para serem inicializadas e a E/S para o armazenamento local do NVMe não é concluída. Se preferir, adicione a seguir linha a `/boot/loader.conf` e reinicialize:

```
hw.nvme.per_cpu_io_queues="0"
```

- O tipo de instância `d2.8xlarge` tem 36 vCPUs, que podem causar problemas de inicialização em alguns sistemas operacionais Linux que têm um limite de 32 vCPUs. Para obter mais informações, consulte [Suporte para vCPUs \(p. 303\)](#).
- 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.

## Linux 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), Field Programmable Gate Arrays (FPGAs) ou AWS Inferentia.

### Tópicos

- [Instâncias de GPU \(p. 306\)](#)
- [Instâncias com o AWS Inferentia \(p. 307\)](#)
- [Instâncias FPGA \(p. 308\)](#)
- [Especificações de hardware \(p. 308\)](#)

- [Da performance da instância \(p. 310\)](#)
- [Performance das redes \(p. 310\)](#)
- [Recursos da instância \(p. 311\)](#)
- [Notas de release \(p. 312\)](#)
- [Instalar drivers NVIDIA nas instâncias do Linux \(p. 313\)](#)
- [Instalar drivers AMD nas instâncias do Linux \(p. 320\)](#)
- [Ativar NVIDIA GRID Virtual Applications \(p. 324\)](#)
- [Para otimizar as configurações de GPU \(p. 325\)](#)

## Instâncias de GPU

As instâncias baseadas em GPU concedem acesso a GPUs NVIDIA com milhares de núcleos de computação. Você pode 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.

### Instâncias G4ad e G4dn

As instâncias G4ad usam GPUs AMD Radeon Pro V520 e processadores AMD EPYC de 2<sup>a</sup> 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 gráficos 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 \(p. 324\)](#).

### 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 P4d

Essas instâncias usam GPUs NVIDIA A100 e fornecem uma plataforma de alta performance para machine learning e workloads HPC. As instâncias P4d oferecem 400 Gbps de taxa de transferência de largura de banda de rede agregada e suporte, Elastic Fabric Adapter (EFA). Elas são as primeiras instâncias do EC2 a fornecer várias placas de rede.

Para obter mais informações, consulte [Instâncias P4d do Amazon EC2](#).

As instâncias P4d são compatíveis com a interconexão NVIDIA NVSwitch GPU e NVIDIA GPUDirect RDMA.

#### 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](#).

## Instâncias com o AWS Inferentia

Estas instâncias foram projetadas para acelerar o machine learning usando o [AWS Inferentia](#), um chip de IA/ML personalizado da Amazon que fornece inferência de machine learning de alta performance e baixa latência. Essas instâncias são otimizadas para implantar modelos de aprendizagem profunda (DL) para aplicações, como processamento de linguagem natural, detecção e classificação de objetos, personalização e filtragem de conteúdo e reconhecimento de fala.

Você pode começar de diversas maneiras:

- Use o SageMaker, um serviço totalmente gerenciado que é a maneira mais fácil de começar a usar modelos de machine learning. Para obter mais informações, consulte [Compilação e implantação de um modelo do TensorFlow no Inf1 usando o Sagemaker Neo](#).
- Execute uma instância Inf1 usando a Deep Learning AMI. Para obter mais informações, consulte [AWS Inferentia with DLAMI](#) (AWS Inferentia com DLAMI) no AWS Deep Learning AMI Developer Guide (Guia do desenvolvedor do AWS Deep Learning AMI).

- Execute uma instância Inf1 usando sua própria AMI e instale o [AWSNeuron SDK](#), que permite compilar, executar e criar perfis de modelos de aprendizagem profunda para AWS Inferentia.
- Execute uma instância de contêiner usando uma instância Inf1 e uma AMI otimizada para Amazon ECS. Para obter mais informações, consulte [AMIs do Amazon Linux 2 \(Inferentia\)](#) no Amazon Elastic Container Service Developer Guide.
- Crie um cluster do Amazon EKS com nós executando instâncias Inf1. Para obter mais informações, consulte [Inferentia support](#) (Suporte para Inferentia) no Amazon EKS User Guide (Manual do usuário do Amazon EKS).

Para obter mais informações, consulte [Machine Learning na AWS](#).

#### Instâncias Inf1

As instâncias Inf1 usam chips de inferência de machine learning do AWS Inferentia. O Inferentia foi desenvolvido para permitir uma performance de inferência altamente econômico e de baixa latência em qualquer escala.

Para obter mais informações, consulte [Instâncias Inf1 do Amazon EC2](#).

## Instâncias FPGA

As instâncias baseadas em FPGA concedem acesso a FPGAs grandes, com milhões de células lógicas de sistema paralelo. Você pode usar instâncias de computação acelerada baseadas em FPGA para acelerar workloads, como análise financeira, genômica, processamento de vídeo em tempo real, análise de big data e workloads de segurança utilizando acelerações de hardware personalizadas. Você pode desenvolver essas acelerações usando linguagens de descrição de hardware, como Verilog ou VHDL, ou usando linguagens de nível superior, como estruturas de computação paralela OpenCL. Você pode desenvolver seu próprio código de aceleração de hardware ou adquirir acelerações de hardware por meio do [AWS Marketplace](#).

A [AMI do desenvolvedor de FPGA](#) fornece as ferramentas para desenvolvimento, teste e criação de AFIs. Você pode usar a AMI de desenvolvedor de FPGA em qualquer instância do EC2 com, pelo menos, 32 GB de memória do sistema (por exemplo, instâncias C5, M4 e R4).

Para obter mais informações, consulte a documentação do [Kit de desenvolvimento de hardware do AWS FPGA](#).

#### Instâncias F1

As instâncias F1 usam FPGAs Xilinx UltraScale+ VU9P e foram projetadas para acelerar algoritmos que usam muita computação, como fluxo de dados ou operações altamente paralelas, não indicadas para CPUs de uso geral. Cada FPGA em uma instância F1 contém aproximadamente 2,5 milhões de elementos de lógica e cerca de 6.800 mecanismos DSP (Processamento de sinal digital), junto com 64 GiB de memória protegida por DDR ECCE local, conectados à instância por uma conexão dedicada PCIe Gen3 x16. As instâncias F1 fornecem volumes SSD NVMe locais.

Os desenvolvedores podem usar o kit do desenvolvedor de hardware da AWS e a AMI do desenvolvedor de FPGA para criar acelerações de hardware personalizadas para uso em instâncias F1. A AMI do desenvolvedor de FPGA inclui ferramentas de desenvolvimento para o desenvolvimento de FPGA de ciclo completo na nuvem. Usando essas ferramentas, os desenvolvedores podem criar e compartilhar imagens de FPGA da Amazon que podem ser carregadas na FPGA de uma instância F1.

Para obter mais informações, consulte [Instâncias F1 do Amazon EC2](#).

## 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
p4d.24xlarge	96	1.152	8
g2.2xlarge	8	15	1
g2.8xlarge	32	60	4
g3s.xlarge	4	30.5	1
g3.4xlarge	16	122	1
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
inf1.xlarge	4	8	1
inf1.2xlarge	8	16	1

Tipo de instância	vCPUs padrão	Memória (GiB)	Aceleradores
inf1.6xlarge	24	48	4
inf1.24xlarge	96	192	16

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 \(p. 616\)](#).

## Da performance da instância

Há várias otimizações de configuração de GPU que você pode executar para obter melhor performance em suas instâncias. Para obter mais informações, consulte [Para otimizar as configurações de GPU \(p. 325\)](#).

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 \(p. 1438\)](#).

Alguns tipos de instância de computação acelerada fornecem a habilidade de controlar C-states do processador e P-states no Linux. Os C-states controlam os níveis de suspensão em que um núcleo pode entrar quando estiver inativo, enquanto os P-states controlam a performance desejada (em frequência da CPU) de um núcleo. Para obter mais informações, consulte [Controle do estado do processo para a instância do EC2 \(p. 604\)](#).

## 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 Linux \(p. 1015\)](#).

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 †	<a href="#">ENA (p. 1016)</a>
g3.8xlarge   p2.8xlarge   p3.8xlarge	10 Gbps	<a href="#">ENA (p. 1016)</a>
g4ad.8xlarge	15 Gbps	<a href="#">ENA (p. 1016)</a>
g4dn.4xlarge e inferior   inf1.2xlarge e inferior	Até 25 Gbps †	<a href="#">ENA (p. 1016)</a>
f1.16xlarge   g3.16xlarge   g4ad.16xlarge	25 Gbps	<a href="#">ENA (p. 1016)</a>

Tipo de instância	Performance das redes	Redes avançadas
<code>inf1.6xlarge   p2.16xlarge   p3.16xlarge</code>		
<code>g4dn.8xlarge   g4dn.12xlarge   g4dn.16xlarge</code>	50 Gbps	<a href="#">ENA (p. 1016)</a>
<code>g4dn.metal   inf1.24xlarge   p3dn.24xlarge</code>	100 Gbps	<a href="#">ENA (p. 1016)</a>
<code>p4d.24xlarge</code>	4x100 Gbps	<a href="#">ENA (p. 1016)</a>

† 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 \(p. 1013\)](#).

Tipo de instância	Largura de banda da linha de base (Gbps)	Largura de banda expandida (Gbps)
<code>g4ad.xlarge</code>	2	10
<code>g4ad.2xlarge</code>	4.167	10
<code>g4ad.4xlarge</code>	8.333	10
<code>g4dn.xlarge</code>	5	25
<code>g4dn.2xlarge</code>	10	25
<code>g4dn.4xlarge</code>	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
G4ad	Não	Sim	NVMe *	Sim
G4dn	Não	Sim	NVMe *	Sim
Inf1	Sim	Não	Não	Sim
P2	Sim	Não	Não	Sim
P3	24xlarge: não	24xlarge: sim	24xlarge: NVMe *	Sim

	Somente EBS	EBS de NVMe	Armazenamento de instâncias	Placement group
	Todos os outros tamanhos: sim	Todos os outros tamanhos: não		
P4d	Não	Sim	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 Linux \(p. 1434\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1494\)](#)
- [Grupos de posicionamento \(p. 1084\)](#)

## Notas de release

- Você deve executar a instância usando uma AMI de HVM.
- As instâncias criadas no [Sistema Nitro \(p. 210\)](#) têm os seguintes requisitos:
  - Os [drivers de NVMe \(p. 1434\)](#) devem estar instalados
  - Os [drivers do Elastic Network Adapter \(ENA\) \(p. 1016\)](#) devem estar instalados

As AMIs do Linux a seguir atendem a esses requisitos:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (com kernel `linux-aws`) ou posterior
- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior
- 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 Linux \(p. 313\)](#).
- 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. O Amazon Linux 2 e as versões mais recentes da AMI do Amazon Linux são compatíveis com PCIe hotplug nativo, mas as versões anteriores não são. Você precisa ativar as seguintes opções de configuração do kernel do Linux:

```
CONFIG_HOTPLUG_PCI_PCIE=y
CONFIG_PCIEASPM=y
```

- 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.

## Instalar drivers NVIDIA nas instâncias do Linux

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 Linux \(p. 320\)](#).

### Sumário

- [Tipos de drivers NVIDIA \(p. 313\)](#)
- [Drivers disponíveis por tipo de instância \(p. 314\)](#)
- [Opções de instalação \(p. 314\)](#)
  - [Opção 1: AMIs com os drivers NVIDIA instalados \(p. 314\)](#)
  - [Opção 2: Drivers NVIDIA públicos \(p. 315\)](#)
  - [Opção 3: drivers GRID \(instâncias G3 e G4dn\) \(p. 315\)](#)
  - [Opção 4: drivers para jogos NVIDIA \(instâncias G4dn\) \(p. 317\)](#)
- [Instalar uma versão adicional do CUDA \(p. 320\)](#)

## 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.

### 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 para Tesla, GRID e drivers de jogos

- 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
P4d	Sim	Não	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 \(p. 314\)](#)
- [Opção 2: Drivers NVIDIA públicos \(p. 315\)](#)
- [Opção 3: drivers GRID \(instâncias G3 e G4dn\) \(p. 315\)](#)
- [Opção 4: drivers para jogos NVIDIA \(instâncias G4dn\) \(p. 317\)](#)

### 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](#)

Para atualizar a versão do driver instalada usando uma dessas AMIs, será necessário desinstalar os pacotes do NVIDIA da instância para evitar conflitos de versão. Use este comando para desinstalar os pacotes do NVIDIA:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

O pacote do toolkit CUDA tem dependências nos drivers NVIDIA. A desinstalação dos pacotes NVIDIA apaga o toolkit CUDA. Você deve reinstalar o toolkit CUDA depois de instalar o driver NVIDIA.

## 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 \(p. 314\)](#). 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 \(p. 315\)](#).

Como fazer download de um driver NVIDIA público

Faça login na instância do Linux 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
P4d	Tesla	A-Series	A100

† As instâncias G4dn requerem a versão de driver 418.87 ou posterior.

Como instalar o driver NVIDIA no Linux

Para obter mais informações sobre como instalar e configurar o driver, consulte o [NVIDIA Driver Installation Quickstart Guide](#).

## Opção 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

- Instale a AWS CLI em sua instância do Linux e configure credenciais padrão. Para obter mais informações, consulte [Installing the AWS CLI](#) (Instalar a AWS CLI) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).
- Os usuários do IAM devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess.

Como instalar o driver NVIDIA GRID na instância do Linux

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.

- Para Amazon Linux, CentOS e Red Hat Enterprise Linux:

```
[ec2-user ~]$ sudo yum update -y
```

- Para Ubuntu e Debian:

```
$ sudo apt-get update -y
```

3. (Ubuntu 16.04 e posterior, com o pacote linux-aws) Atualize o pacote linux-aws para receber a versão mais recente.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.
6. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

- Para Amazon Linux, CentOS e Red Hat Enterprise Linux:

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

- Para Ubuntu e Debian:

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

7. [CentOS, Red Hat Enterprise Linux, Ubuntu, Debian] Desabilite o driver de código aberto nouveau para placas gráficas NVIDIA.

- a. Adicione o nouveau ao arquivo de lista de proibição /etc/modprobe.d/blacklist.conf. Copie o bloco de código a seguir e cole-o em um terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivaafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- b. Edite o arquivo /etc/default/grub e adicione a linha a seguir:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- c. Recompile a configuração do Grub.

- Para CentOS e Red Hat Enterprise Linux:

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

- Para Ubuntu e Debian:

```
$ sudo update-grub
```

- Faça download do utilitário de instalação do driver GRID usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Várias versões de driver GRID são armazenadas nesse bucket. Você pode visualizar todas as versões disponíveis usando o comando a seguir.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

Começando com o GRID versão 11.0, você pode usar os pacotes de driver no `latest` para as 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`.

- Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

- Execute o script de autoinstalação conforme segue para instalar o driver GRID baixado. Por exemplo:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (você pode aceitar as opções padrão).

- Reinicie a instância.

```
[ec2-user ~]$ sudo reboot
```

- Verifique se o driver está funcionando. A resposta para o comando a seguir lista a versão instalada do driver NVIDIA e os detalhes das GPUs.

```
[ec2-user ~]$ nvidia-smi -q | head
```

- (Opcional) Dependendo do seu caso de uso, você pode concluir as seguintes etapas opcionais. Se você não precisar dessa funcionalidade, não conclua essas etapas.

- Para ajudar a beneficiar-se dos quatro monitores com resolução de até 4 K, configure o protocolo de exibição de alta performance, [NICE DCV](#).
- O modo NVIDIA Quadro Virtual Workstation é habilitado por padrão. Para ativar as aplicações virtuais GRID para recursos de hospedagem de aplicações RDSH, conclua as etapas de ativação da aplicação virtual GRID em [Ativar NVIDIA GRID Virtual Applications \(p. 324\)](#).

#### 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

- Instale a AWS CLI em sua instância do Linux e configure credenciais padrão. Para obter mais informações, consulte [Installing the AWS CLI](#) (Instalar a AWS CLI) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).
- Os usuários do IAM devem ter as permissões concedidas pela política `AmazonS3ReadOnlyAccess`.

### Como instalar o driver para jogos NVIDIA na instância do Linux

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.
  - Para Amazon Linux, CentOS e Red Hat Enterprise Linux:

```
[ec2-user ~]$ sudo yum update -y
```

- Para Ubuntu e Debian:

```
$ sudo apt-get update -y
```

3. (Ubuntu 16.04 e posterior, com o pacote linux-aws) Atualize o pacote linux-aws para receber a versão mais recente.

```
$ sudo apt-get upgrade -y linux-aws
```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
[ec2-user ~]$ sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.
6. Instale o compilador gcc e o pacote os cabeçalhos para a versão do kernel que você está executando atualmente.

- Para Amazon Linux, CentOS e Red Hat Enterprise Linux:

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

- Para Ubuntu e Debian:

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

7. [CentOS, Red Hat Enterprise Linux, Ubuntu, Debian] Desabilite o driver de código aberto nouveau para placas gráficas NVIDIA.

- a. Adicione o nouveau ao arquivo de lista de proibição /etc/modprobe.d/blacklist.conf. Copie o bloco de código a seguir e cole-o em um terminal.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- b. Edite o arquivo /etc/default/grub e adicione a linha a seguir:

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- c. Recompile a configuração do Grub.

- Para CentOS e Red Hat Enterprise Linux:

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

- Para Ubuntu e Debian:

```
$ sudo update-grub
```

8. Baixe o utilitário de instalação do driver para jogos usando o comando a seguir:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Muitas versões do driver para jogos são armazenadas neste bucket. Você pode visualizar todas as versões disponíveis usando o comando a seguir:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Adicione as permissões para executar o utilitário de instalação do driver usando o comando a seguir.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Execute o instalador usando o comando a seguir:

```
[ec2-user ~]$ sudo ./NVIDIA-Linux-x86_64*.run
```

Quando solicitado, aceite o acordo de licença e especifique as opções de instalação conforme o necessário (você pode aceitar as opções padrão).

11. Use o comando a seguir para criar o arquivo de configuração necessário.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Use o comando a seguir para fazer download e renomear o arquivo de certificação.

- Para a versão 460.39 ou posterior:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2021_10_2.cert"
```

- Para versões de 440.68 a 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

- Para versões anteriores

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

13. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

14. (Opcional) Para ajudar a aproveitar um 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 Linux.
2. Abra o [site da NVIDIA](#) e selecione a versão do CUDA que você precisa.
3. Selecione a arquitetura, a distribuição e a versão do sistema operacional em sua instância. Em Installer Type (Tipo de instalador), selecione runfile (local).
4. Siga as instruções para fazer download do script de instalação.
5. Adicione permissões de execução ao script de instalação que você obteve por download usando o comando a seguir.

```
[ec2-user ~]$ chmod +x downloaded_installer_file
```

6. Execute o script de instalação como mostrado a seguir para instalar o toolkit do CUDA e adicionar o número da versão do CUDA ao caminho do toolkit.

```
[ec2-user ~]$ sudo downloaded_installer_file --silent --override --toolkit --samples --  
toolkitpath=/usr/local/cuda-version --samplespath=/usr/local/cuda --no-opengl-lib
```

7. (Opcional) Defina a versão padrão do CUDA da seguinte forma.

```
[ec2-user ~]$ ln -s /usr/local/cuda-version /usr/local/cuda
```

## Instalar drivers AMD nas instâncias do Linux

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 Linux \(p. 313\)](#).

### Sumário

- [Software AMD Radeon Pro para driver empresarial \(p. 320\)](#)
- [AMIs com o driver AMD instalado \(p. 321\)](#)
- [Download do driver AMD \(p. 321\)](#)
- [Configurar um desktop interativo \(p. 322\)](#)

## 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

- Framework de mídia avançada da AMD
- API de aceleração de vídeo

## 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

- Instale a AWS CLI em sua instância do Linux e configure credenciais padrão. Para obter mais informações, consulte [Installing the AWS CLI](#) (Instalar a AWS CLI) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).
- Os usuários do IAM devem ter as permissões concedidas pela política AmazonS3ReadOnlyAccess.

### Para instalar o driver AMD em sua instância do Linux

1. Conecte-se à sua instância do Linux. Instale gcc e make, caso ainda não tenham sido instalados.
2. Atualize o cache de pacotes e obtenha as atualizações de pacotes para sua instância.
  - Para Amazon Linux 2:

```
$ sudo amazon-linux-extras install epel -y
$ sudo yum update -y
```

- Para o Ubuntu:

```
$ sudo dpkg --add-architecture i386
$ sudo apt-get update -y && sudo apt upgrade -y
```

- Para o CentOS:

```
$ sudo yum install epel-release -y
$ sudo yum update -y
```

3. Reinicialize a instância.

```
$ sudo reboot
```

4. Reconecte-se à instância depois que ela for reinicializada.
5. Faça download do driver AMD mais recente.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

6. Extraia o arquivo.

- Para Amazon Linux 2 e CentOS:

```
$ tar -xf amdgpu-pro-*rhel*.tar.xz
```

- Para o Ubuntu:

```
$ tar -xf amdgpu-pro*ubuntu*.xz
```

7. Mude para a pasta do driver extraído.
8. Adicione as chaves GPG para a instalação do driver.

- Para Amazon Linux 2 e CentOS:

```
$ sudo rpm --import RPM-GPG-KEY-amdgpu
```

- Para o Ubuntu:

```
$ sudo apt install linux-modules-extra-$(uname -r) -y
$ cat RPM-GPG-KEY-amdgpu | sudo apt-key add -
```

9. Execute o script de instalação automática para instalar a pilha completa de gráficos.

```
$ ./amdgpu-pro-install -y --opencl=pal,legacy
```

10. Reinicie a instância.

```
$ sudo reboot
```

11. Verifique se o driver está funcionando.

```
$ dmesg | grep amdgpu
```

A resposta deve ser parecida com o seguinte:

```
Initialized amdgpu
```

## Configurar um desktop interativo

Depois de confirmar se a instância tem o driver da GPU AMD instalado e se o amdgpu está em uso, você pode instalar um gerenciador de desktop interativo. Recomendamos o ambiente de desktop MATE para obter a melhor compatibilidade e performance.

### Prerequisite

Abra um editor de texto e salve o seguinte como um arquivo chamado `xorg.conf`. Você precisará desse arquivo em sua instância.

```
Section "ServerLayout"
    Identifier      "Layout0"
    Screen          0 "Screen0"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
    ModulePath     "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath     "/opt/amdgpu/lib/xorg/modules"
```

```
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier      "Mouse0"
    Driver          "mouse"
    Option          "Protocol" "auto"
    Option          "Device"   "/dev/psaux"
    Option          "Emulate3Buttons" "no"
    Option          "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier      "Keyboard0"
    Driver          "kbd"
EndSection
Section "Monitor"
    Identifier      "Monitor0"
    VendorName     "Unknown"
    ModelName      "Unknown"
EndSection
Section "Device"
    Identifier      "Device0"
    Driver          "amdgpu"
    VendorName     "AMD"
    BoardName       "Radeon Rx GPU V520"
    BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
    Option          "DPMS" "Disable"
EndSection
Section "Screen"
    Identifier      "Screen0"
    Device          "Device0"
    Monitor         "Monitor0"
    DefaultDepth    24
    Option          "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual        3840 2160
        Depth          32
    EndSubSection
EndSection
EndSection
```

Para configurar um desktop interativo no Amazon Linux 2

1. Instale o repositório EPEL.

```
$ sudo amazon-linux-extras install epel -y
```

2. Instale o desktop MATE.

```
$ sudo amazon-linux-extras install mate-desktop1.x -y
$ sudo yum groupinstall "MATE Desktop" -y
$ sudo systemctl disable firewalld
```

3. Copie o arquivo xorg.conf para /etc/X11/xorg.conf.
4. Reinicie a instância.

```
$ sudo reboot
```

5. (Opcional) [Instale o servidor NICE DCV](#) para usar NICE DCV como um protocolo de exibição de alta performance e, em seguida, [conecte-se a uma sessão NICE DCV](#) usando seu cliente preferido.

Para configurar um desktop interativo no Ubuntu

1. Instale o desktop MATE.

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y  
$ sudo apt purge ifupdown -y
```

2. Copie o arquivo xorg.conf para /etc/X11/xorg.conf.
3. Reinicialize a instância.

```
$ sudo reboot
```

4. Instale o codificador AMF para a versão apropriada do Ubuntu.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Opcional) [Instale o servidor NICE DCV](#) para usar NICE DCV como um protocolo de exibição de alta performance e, em seguida, [conecte-se a uma sessão NICE DCV](#) usando seu cliente preferido.
6. Após a instalação do DCV, dê permissões de vídeo ao usuário DCV:

```
$ sudo usermod -aG video dcv
```

Para configurar um desktop interativo no CentOS

1. Instale o repositório EPEL.

```
$ sudo yum update -y  
$ sudo yum install epel-release -y
```

2. Instale o desktop MATE.

```
$ sudo yum groupinstall "MATE Desktop" -y  
$ sudo systemctl disable firewalld
```

3. Copie o arquivo xorg.conf para /etc/X11/xorg.conf.
4. Reinicialize a instância.

```
$ sudo reboot
```

5. (Opcional) [Instale o servidor NICE DCV](#) para usar NICE DCV como um protocolo de exibição de alta performance e, em seguida, [conecte-se a uma sessão NICE DCV](#) usando seu cliente preferido.

## 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 arquivo /etc/nvidia/gridd.conf .

Como ativar GRID Virtual Applications nas instâncias do Linux

1. Crie o arquivo /etc/nvidia/gridd.conf a partir do arquivo de modelo fornecido.

```
[ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
```

2. Abra o arquivo /etc/nvidia/gridd.conf no editor de texto favorito.
3. Localize a linha FeatureType e defina-a como igual a 0. Em seguida, adicione uma linha com IgnoreSP=TRUE.

```
FeatureType=0
IgnoreSP=TRUE
```

4. Salve o arquivo e saia.
5. Reinicie a instância para obter a nova configuração.

```
[ec2-user ~]$ sudo reboot
```

## 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 P3dn, e P4d. 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. O procedimento a seguir ajuda a configurar as definições de GPU para serem persistentes, desabilitar o recurso de autoboot e definir as velocidades de clock de GPU como a frequência máxima.

### Para otimizar as configurações de GPU

1. Defina as configurações de GPU para serem persistentes. Esse comando pode levar vários minutos para ser executado.

```
[ec2-user ~]$ sudo nvidia-persistenced
```

2. Instâncias G2, G3 e P2: desative o recurso de autoboot para todas as GPUs na instância.

#### Note

GPUs em instâncias G4dn, P3 P3dn, e P4d não oferecem suporte a autoboot.

```
[ec2-user ~]$ sudo 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:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
```

- Instâncias G4dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
```

- Instâncias P2:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2505,875
```

- Instâncias P3 e P3dn:

```
[ec2-user ~]$ sudo nvidia-smi -ac 877,1530
```

- Instâncias P4d:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

## 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. \(p. 510\)](#).

## 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
```

4. 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 \(p. 334\)](#).

### Tópicos

- [Requisitos para alterar os tipos de instância \(p. 327\)](#)
- [Compatibilidade para alterar o tipo de instância \(p. 328\)](#)
- [Alterar o tipo de instância de uma instância com Amazon EBS \(p. 329\)](#)
- [Migrar uma instância com suporte de armazenamento de instâncias \(p. 331\)](#)
- [Migrar para uma nova configuração de instância \(p. 332\)](#)

## Requisitos para alterar os tipos de instância

Para redimensionar a instância do Amazon EC2 alterando o tipo de instância, considere os seguintes requisitos:

- As etapas para alterar o tipo de instância são diferentes, variando se a propriedade [volume raiz \(p. 1521\)](#) da instância é um volume do EBS ou um volume de armazenamento de instâncias.
  - Se o dispositivo raiz estiver em um volume do EBS, você poderá alterar o tipo de instância da instância original. Para obter instruções, consulte [Alterar o tipo de instância de uma instância com Amazon EBS \(p. 329\)](#).
  - Se o dispositivo raiz estiver em um volume de armazenamento de instâncias, você deverá migrar a aplicação para uma nova instância que esteja configurada com o tipo de instância necessário. Para obter instruções, consulte [Migrar uma instância com suporte de armazenamento de instâncias \(p. 331\)](#)
- 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:

- Tipo de virtualização: as AMIs do Linux usam um dos dois tipos de virtualização, Paravirtual (PV) ou Hardware Virtual Machine (HVM – Máquina virtual de hardware). Você não pode redimensionar uma instância que seja executada em uma AMI PV para um tipo de instância que seja HVM somente. Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#). Para verificar o tipo de virtualização da instância, consulte o campo `Virtualization` no painel de detalhes da tela `Instances` no console do Amazon EC2.
- 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 \(p. 1120\)](#).
- Redes aprimoradas: tipos de instância que dão suporte a [redes aprimoradas \(p. 1015\)](#) exigem os drivers necessários instalados. Por exemplo, as instâncias baseadas no [Sistema Nitro \(p. 210\)](#) 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 \(p. 1016\)](#) ou os [drivers ixgbevf \(p. 1026\)](#) na instância, conforme apropriado.
- Placas de rede: alguns tipos de instância são compatíveis com [várias placas de rede \(p. 986\)](#). Você deve selecionar um tipo de instância que ofereça suporte ao mesmo número de placas de rede que o tipo de instância atual.
- NVMe: os volumes do EBS são expostos como dispositivos de blocos NVMe em instâncias criadas no [sistema Nitro \(p. 210\)](#). 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. 1434](#)) 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`). Portanto, para montar sistemas de arquivos no momento da inicialização usando `/etc/fstab`, você deve usar UUID/Label ao invés de nomes de dispositivos.

- 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 \(p. 214\)](#)
  - [Instâncias otimizadas para computação \(p. 273\)](#)
  - [Instâncias otimizadas para memória \(p. 282\)](#)
  - [Instâncias otimizadas para armazenamento \(p. 297\)](#)

## 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 \(p. 1085\)](#) 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 \(p. 562\)](#).

### 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 \(p. 328\)](#).
2. Abra o console do Amazon EC2.
3. No painel de navegação, escolha Instances (Instâncias).
4. Selecione a instância e escolha Actions (Ações), Instance state (Estado da instância) e Stop instance (Interromper instância).
5. Na caixa de diálogo de confirmação, escolha Stop (Interromper). Pode demorar alguns minutos para que a instância pare.
6. 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.
7. 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 \(p. 328\)](#).
  - 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.
8. 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.
9. (Solução de problemas) Se a sua instância não inicializar, é possível que um dos requisitos para o novo tipo de instância não tenha sido atendido. Para obter mais informações, consulte [Por que minha instância Linux não está inicializando depois que mudei seu tipo?](#)

## 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 \(p. 328\)](#).
2. Abra o console do Amazon EC2.
3. No painel de navegação, escolha Instances (Instâncias).
4. Selecione a instância e escolha Actions, Instance State e Stop.
5. Na caixa de diálogo para confirmação, escolha Yes, parar. Pode demorar alguns minutos para que a instância pare.
6. Com a instância ainda selecionada, escolha Ações, Instance Settings, Change Instance Type. Essa ação estará acinzentada se o estado da instância não for stopped.
7. 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 \(p. 328\)](#).

- b. (Opcional) Se o tipo de instância selecionado oferecer suporte a otimização para EBS, selecione EBS-optimized (Otimizado para EBS) ou desmarque a opção EBS-optimized (Otimizado para EBS) para desativar a otimização para EBS. Se, por padrão, o tipo de instância selecionado for otimizada para EBS, a opção EBS-optimized (Otimizada para EBS) estará selecionada e você não poderá desmarcá-la.
- c. Escolha Apply para aceitar as novas configurações.
8. Para reiniciar a instância interrompida, selecione a instância e escolha Ações, Instance State, Iniciar.
9. Na caixa de diálogo de confirmação, escolha Sim, iniciar. Pode demorar alguns minutos para que a instância entre no estado `running`.
10. (Solução de problemas) Se a sua instância não inicializar, é possível que um dos requisitos para o novo tipo de instância não tenha sido atendido. Para obter mais informações, consulte [Por que minha instância Linux não está inicializando depois que mudei seu tipo?](#)

## Migrar uma instância com suporte de armazenamento de instâncias

Você não pode alterar o tipo de instância de uma instância de armazenamento de instância. Em vez disso, você deverá migrar a aplicação para uma nova instância que esteja configurada com o tipo de instância necessário. Para migrar a aplicação para uma nova instância, você deve criar uma imagem da instância original e iniciar uma nova instância dessa imagem com o tipo de instância necessário. Para garantir que os usuários possam continuar usando as aplicações que você está hospedando em sua instância sem interrupção, você deve usar qualquer endereço IP elástico associado à instância original e associá-lo à nova instância. Em seguida, é possível encerrar a instância original.

New console

### Para migrar uma instância com suporte de armazenamento de instâncias

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, faça um snapshot dos volumes (veja [Criar snapshots de Amazon EBS \(p. 1307\)](#)) 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 Linux \(p. 1300\)](#)).
2. Crie uma AMI de sua instância com suporte do armazenamento de instâncias atendendo aos pré-requisitos e seguindo os procedimentos em [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#). Ao concluir a criação de uma AMI de sua instância, retorne para esse procedimento.
3. Abra o console do Amazon EC2 e, no painel de navegação, selecione AMIs. Na lista de filtros, selecione Owned by me (De minha propriedade) e selecione a imagem que você criou na etapa anterior. Observe que o AMI Name é o nome que você especificou quando registrou a imagem e Source é seu bucket do Amazon S3.

#### Note

Se você não vir a AMI criada na etapa anterior, verifique se selecionou a região na qual criou a AMI.

4. Escolha Executar. Ao especificar opções para a instância, selecione o novo tipo de instância desejado. Se o tipo de instância desejado não puder ser selecionado, ele não será compatível com a configuração da AMI criada (por exemplo, devido ao tipo de virtualização). Você também pode especificar todos os volumes do EBS que desanexou da instância original.

Pode demorar alguns minutos para que a instância entre no estado `running`.

5. (Opcional) Você pode encerrar a instância com a qual começou 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 uma instância com suporte de armazenamento de instâncias

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, faça um snapshot dos volumes (veja [Criar snapshots de Amazon EBS \(p. 1307\)](#)) 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 Linux \(p. 1300\)](#)).
2. Crie uma AMI de sua instância com suporte do armazenamento de instâncias atendendo aos pré-requisitos e seguindo os procedimentos em [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#). Ao concluir a criação de uma AMI de sua instância, retorne para esse procedimento.
3. Abra o console do Amazon EC2 e, no painel de navegação, selecione AMIs. Na lista de filtros, selecione Owned by me (De minha propriedade) e selecione a imagem que você criou na etapa anterior. Observe que o AMI Name é o nome que você especificou quando registrou a imagem e Source é seu bucket do Amazon S3.

#### Note

Se você não vir a AMI criada na etapa anterior, verifique se selecionou a região na qual criou a AMI.

4. Escolha Executar. Ao especificar opções para a instância, selecione o novo tipo de instância desejado. Se o tipo de instância desejado não puder ser selecionado, ele não será compatível com a configuração da AMI criada (por exemplo, devido ao tipo de virtualização). Você também pode especificar todos os volumes do EBS que desanexou da instância original.

Pode demorar alguns minutos para que a instância entre no estado `running`.

5. (Opcional) Você pode encerrar a instância com a qual começou 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).

## 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.

Para mover de uma instância executada em uma AMI PV para um tipo de instância que seja HVM somente, o processo geral é o seguinte:

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 \(p. 1307\)](#))

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 Linux \(p. 1300\)](#)).

2. Execute uma nova instância selecionando o seguinte:
  - Uma AMI de HVM.
  - O tipo de instância HVM somente.
  - 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 \(p. 1307\)](#)) 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 Linux \(p. 1300\)](#)).
2. Execute uma nova instância selecionando o seguinte:
  - Uma AMI de HVM.
  - O tipo de instância HVM somente.
  - 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 \(p. 334\)](#)
- [Findings \(p. 335\)](#)
- [Exibir recomendações \(p. 335\)](#)
- [Considerações para avaliação das recomendações \(p. 337\)](#)
- [Recursos adicionais \(p. 337\)](#)

## 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 \(p. 203\)](#).

## 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 \(p. 334\)](#) 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 \(p. 230\)](#).
- 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 \(p. 328\)](#).
- 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 \(p. 327\)](#).

## Recursos adicionais

Para obter mais informações:

- [Tipos de instância \(p. 203\)](#)
- [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 \(p. 338\)](#)
- [On-Demand Instances \(p. 340\)](#)
- [Reserved Instances \(p. 343\)](#)
- [Scheduled Reserved Instances \(p. 387\)](#)
- [Spot Instances \(p. 389\)](#)
- [Dedicated Hosts \(p. 440\)](#)
- [Dedicated Instances \(p. 475\)](#)
- [On-Demand Capacity Reservations \(p. 481\)](#)

## 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 \(p. 1567\)](#).

## 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 \(p. 1567\)](#).

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 segunda , 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 segundos que suas Instâncias on-demand estiverem no estado `running`. O preço por segundo 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. 389) ou [Reserved Instances](#) (p. 343).

### Sumário

- [Trabalhar com Instâncias on-demand](#) (p. 340)
- [Limites de instância sob demanda](#) (p. 340)
  - [Calcular quantas vCPUs você precisa](#) (p. 341)
  - [Solicitar um aumento de limite de](#) (p. 343)
  - [Monitorar limites e uso de instância sob demanda](#) (p. 343)
- [Consulte os preços das instâncias sob demanda](#) (p. 343)

## Trabalhar com Instâncias on-demand

Você pode trabalhar com Instâncias on-demand das seguintes formas:

- [Executar sua instância](#) (p. 509)
- [Conecte-se à sua instância do Linux](#) (p. 535)
- [Interromper e iniciar sua instância](#) (p. 562)
- [Hibernar a instância do Windows sob demanda ou reservada](#) (p. 566)
- [Reinicializar a instância](#) (p. 583)
- [Desativação da instância](#) (p. 584)
- [Encerrar a instância](#) (p. 587)
- [Recuperar a instância](#) (p. 593)
- [Configurar sua instância do Amazon Linux](#) (p. 595)
- [Identificar as instâncias do Linux do EC2](#) (p. 698)

Se você é novo com o Amazon EC2, consulte [Como começar a usar o Amazon EC2](#) (p. 1).

## 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.

**Limits Calculator**  
Use this tool to calculate how many vCPUs you need to launch your On-Demand Instances

Select the instance type and the number of instances you require. The calculator will display the number of vCPUs assigned to the selected instances. Use the New Limit value as a guide for requesting a limit increase.

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

[Add instance type](#)

**Limits calculation**

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	<a href="#">Request limit increase</a>
All F instances	176 vCPUs	128 vCPUs	304 vCPUs	<a href="#">Request limit increase</a>

[Close](#)

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 \(p. 1565\)](#).

### 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 \(p. 1565\)](#) 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 Manual do usuário do Service Quotas.

### 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.

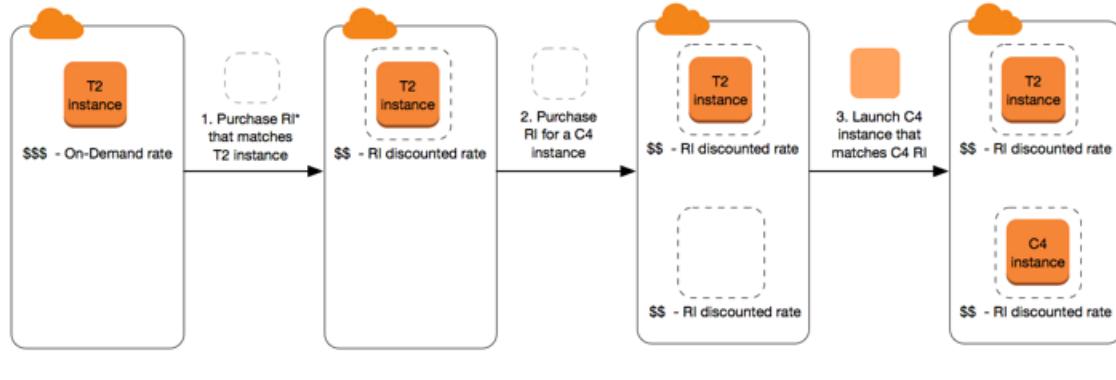
O Savings Plans também oferece economias significativas nos custos do Amazon EC2 comparado à definição de preço de instância sob demanda. Com o Savings Plans, você se compromete com uma quantidade consistente de uso, medida em USD por hora. Isso oferece a flexibilidade de usar as configurações de instância 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 \(p. 344\)](#)
- [Principais variáveis que determinam a definição de preço da Instância reservada \(p. 345\)](#)
- [Limites de Instância reservada \(p. 346\)](#)
- [Instâncias reservadas regionais e zonais \(escopo\) \(p. 347\)](#)
- [Tipos de Instâncias reservadas \(classes de oferta\) \(p. 348\)](#)
- [Como as Instâncias reservadas são aplicadas \(p. 348\)](#)
- [Use as suas Instâncias reservadas \(p. 354\)](#)
- [Como você é cobrado \(p. 354\)](#)
- [Comprar Instâncias reservadas \(p. 359\)](#)
- [Vender no Marketplace de instâncias reservadas \(p. 368\)](#)
- [Modificar a Instâncias reservadas \(p. 375\)](#)
- [Trocá Instâncias reservadas conversíveis \(p. 383\)](#)

## 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 \(p. 475\)](#).
- Plataforma: O sistema operacional; por exemplo, Windows ou Linux/Unix. Para obter mais informações, consulte [Escolher uma plataforma \(p. 360\)](#).

### 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 \(p. 368\)](#).

## 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 \(classes de oferta\) \(p. 348\)](#).

Após adquirir uma Instância reservada, você não poderá cancelar a compra. Contudo, você poderá [modificar \(p. 375\)](#), [trocar \(p. 383\)](#) ou [vender \(p. 368\)](#) 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 \(p. 349\)](#) por mês além de um adicional de 20 Instâncias reservadas [zonais \(p. 348\)](#) 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 \(p. 1565\)](#).

## 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 \(p. 345\)](#) 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 <a href="#">Flexibilidade de tamanho da instância determinada pelo fator de normalização (p. 349)</a> .	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 \(p. 348\)](#).

## 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 as 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 <a href="#">Modificar a Instâncias reservadas (p. 375)</a> .	Alguns atributos podem ser modificados. Para obter mais informações, consulte <a href="#">Modificar a Instâncias reservadas (p. 375)</a> .
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 <a href="#">Trocar Instâncias reservadas conversíveis (p. 383)</a> .
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 \(p. 354\)](#).

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.

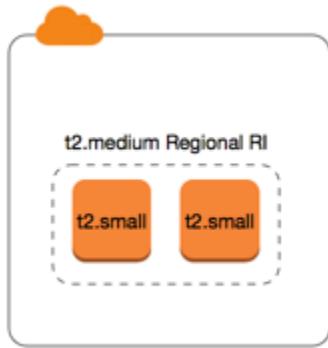
A flexibilidade do tamanho da instância é aplicada do menor para o maior tamanho de instância na família de instâncias com base no fator de normalização.

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.

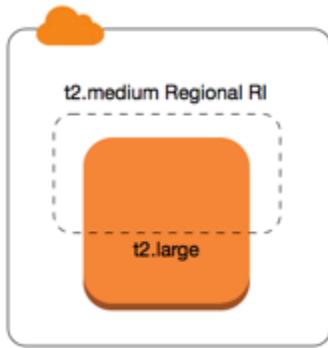
Tamanho da instância	Fator de normalização
nano	0.25
micro	0,5
small	1
medium	2
large	4
xlarge	8
2xlarge	16

Tamanho da instância	Fator de normalização
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 \(p. 375\)](#).

#### 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>a1.metal</code>	32
<code>m5zn.metal</code>   <code>z1d.metal</code>	96
<code>c6g.metal</code>   <code>c6gd.metal</code>   <code>i3.metal</code>   <code>m6g.metal</code>   <code>m6gd.metal</code>   <code>r6g.metal</code>   <code>r6gd.metal</code>   <code>x2gd.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 \(p. 357\)](#). 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 Instâncias 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 \(p. 475\)](#).

Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 510\)](#). Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte [Como as Instâncias reservadas são aplicadas \(p. 348\)](#).

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 \(p. 345\)](#) 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 \(p. 360\)](#).

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 \(p. 355\)](#)
- [Visualizar sua fatura \(p. 356\)](#)
- [Instâncias reservadas e faturamento consolidado \(p. 357\)](#)
- [Níveis de definição de preço com desconto da Instância reservada \(p. 357\)](#)

## 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 \(p. 503\)](#).

Um benefício do faturamento de Instância reservada pode ser aplicado a uma instância em execução com base em uma taxa por segundo. O faturamento por segundo está disponível para instâncias que usam uma distribuição de código aberto do Linux, como o Amazon Linux e o Ubuntu. O faturamento por hora é usado para distribuições comerciais do Linux, como o Red Hat Enterprise Linux e o SUSE Linux Enterprise Server.

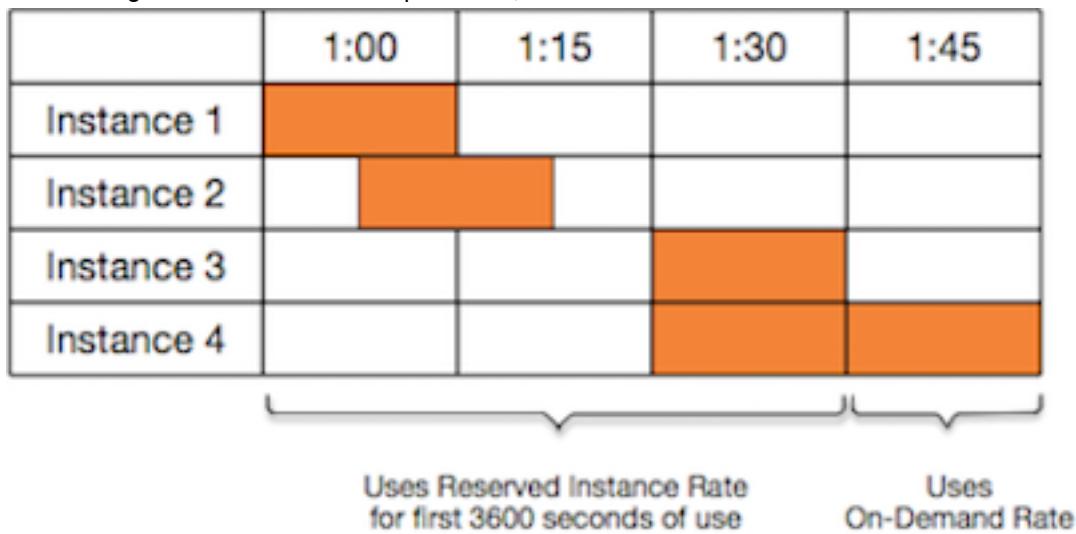
Um dos benefícios de faturamento da Instância reservada pode ser aplicado a um máximo de 3600 segundos (uma hora) de uso de instância por hora fechada. Você pode executar várias instâncias simultaneamente, mas só pode receber o benefício do desconto de Instância reservada por um total de 3600 segundos 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 \(p. 357\)](#)
- [Comprar com nível de desconto \(p. 358\)](#)
- [Cruzamento de níveis de definição de preço \(p. 359\)](#)
- [Faturamento consolidado para níveis de definição de preço \(p. 359\)](#)

### 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 \(p. 359\)](#).

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 \(p. 359\)](#).

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 de desconto inferior e as reservas restantes com a taxa de 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 \(p. 357\)](#).

## 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 procura 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 \(p. 360\)](#)
- [Enfileirar sua compra \(p. 360\)](#)
- [Comprar Instâncias reservadas padrão \(p. 361\)](#)
- [Comprar Instâncias reservadas conversíveis \(p. 364\)](#)
- [Comprar do Marketplace da Instância reservada \(p. 366\)](#)
- [Como exibir o Instâncias reservadas \(p. 367\)](#)
- [Como cancelar uma compra colocada na fila \(p. 367\)](#)
- [Renovar uma Instância reservada \(p. 368\)](#)

## Escolher uma plataforma

O Amazon EC2 é compatível com as seguintes plataformas Linux para Instâncias reservadas:

- Linux/UNIX
- Linux com SQL Server Standard
- Linux com SQL Server Web
- Linux com SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux com HA

Quando adquire uma Instância reservada, você deve escolher uma oferta para uma plataforma que represente o sistema operacional da sua instância.

- Para as distribuições do SUSE Linux e do RHEL, é necessário escolher ofertas para essas plataformas específicas, ou seja, para as plataformas SUSE Linux ou Red Hat Enterprise Linux.
- Para todas as demais distribuições do Linux (incluindo Ubuntu), escolha uma oferta para a plataforma Linux/UNIX.
- Se você trouxer sua assinatura de RHEL existente, será necessário escolher uma oferta para a plataforma Linux/UNIX, não uma oferta para a plataforma Red Hat Enterprise Linux.

#### 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 do Instância reservada, caso contrário, o 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 \(p. 168\)](#).

Para obter informações sobre as plataformas compatíveis com Windows, consulte [Como escolher uma plataforma](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## 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 \(p. 367\)](#).

## 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 \(p. 366\)](#).

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=3153600 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 \(p. 354\)](#).

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte [Como as Instâncias reservadas são aplicadas \(p. 348\)](#).

## 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 reservedas (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 Instances reservedas (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 \(p. 354\)](#).

Para obter exemplos de como as Instâncias reservadas são aplicadas às instâncias em execução, consulte [Como as Instâncias reservadas são aplicadas \(p. 348\)](#).

## 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 \(p. 361\)](#).

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 \(p. 368\)](#). Para obter mais informações, consulte [Estados de listagem da Instância reservada \(p. 373\)](#).

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 \(p. 366\)](#).

#### Tópicos

- [Restrições e limitações \(p. 369\)](#)
- [Registre-se como vendedor \(p. 370\)](#)
- [Conta de banco para desembolso \(p. 370\)](#)
- [Informações fiscais \(p. 371\)](#)
- [Precificar suas Instâncias reservadas \(p. 371\)](#)
- [Liste as suas Instâncias reservadas \(p. 372\)](#)
- [Estados de listagem da Instância reservada \(p. 373\)](#)
- [Ciclo de vida de uma lista \(p. 373\)](#)
- [Depois que a Instância reservada é vendida \(p. 374\)](#)
- [Recebimentos \(p. 374\)](#)
- [Informações compartilhadas com o comprador \(p. 374\)](#)

## 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 \(p. 370\)](#).

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 \(p. 371\)](#). Você também pode modificar as Instâncias reservadas antes de listá-las. Para obter mais informações, consulte [Modificar a Instâncias reservadas \(p. 375\)](#).
- 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 \(p. 370\)](#).
- 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 \(p. 371\)](#).

Após a AWS receber o registro preenchido do vendedor, você receber um e-mail confirmando 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 , tamanho da instância (dentro da mesma família de instâncias), 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 [Trocar Instâncias reservadas conversíveis \(p. 383\)](#).

Você pode modificar todas as Instâncias reservadas ou um subconjunto delas. Você pode separar suas Instâncias reservadas originais em duas ou mais novas Instâncias reservadas. Por exemplo, se você tiver uma reserva de 10 instâncias em us-east-1a e decidir mover 5 instâncias para us-east-1b, a solicitação da modificação resultará em duas novas reservas: uma para 5 instâncias em us-east-1a e outra para as outras 5 instâncias em us-east-1b.

Você também pode mesclar duas ou mais Instâncias reservadas em uma única Instância reservada. Por exemplo, se você tiver quatro t2.small Instâncias reservadas de uma instância cada, poderá mesclá-las para criar uma t2.large Instância reservada. Para obter mais informações, consulte [Suporte para modificar tamanhos de instância \(p. 377\)](#).

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 \(p. 376\)](#)
- [Suporte para modificar tamanhos de instância \(p. 377\)](#)
- [Enviar solicitações de modificação \(p. 380\)](#)
- [Soluçinar problemas de solicitações de modificação \(p. 382\)](#)

## 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 <a href="#">Como as Instâncias reservadas são aplicadas (p. 348)</a>.</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 <a href="#">Suporte para modificar tamanhos de instância (p. 377)</a> .
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

Atributo modificável	Plataformas compatíveis	Limitações
		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
- Deve haver correspondência entre o tamanho ocupado pela instância da reserva original e a nova configuração. Para obter mais informações, consulte [Suporte para modificar tamanhos de instância \(p. 377\)](#).
- 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.

## Suporte para modificar tamanhos de instância

Você pode modificar o tamanho da instância de um Instância reservada se os seguintes requisitos forem atendidos.

## Requirements

- A plataforma é Linux/UNIX.
- Você deve selecionar outro tamanho de instância na mesma família de instâncias. Por exemplo, você não pode modificar um Instância reservada de t2 para t3, sejam os tamanhos iguais ou diferentes.

Não é possível modificar o tamanho da instância de Instâncias reservadas para as seguintes instâncias, porque cada uma dessas famílias de instâncias tem apenas um tamanho:

- cc2.8xlarge
- cr1.8xlarge
- hs1.8xlarge
- t1.micro
- As Instância reservada original e modificada devem ter o mesmo espaço para tamanho de instância.

## Tópicos

- [Espaço para tamanho da instância \(p. 377\)](#)
- [Fatores de normalização para instâncias bare metal \(p. 379\)](#)

## Espaço para tamanho da instância

Cada Instância reservada tem um espaço para tamanho da instância, que é determinado pelo fator de normalização do tamanho de instância e pelo número de instâncias na reserva. Ao modificar os tamanhos

da instância em uma Instância reservada, o espaço da nova configuração deverá ser equivalente ao da configuração original; caso contrário, a solicitação de modificação não será processada.

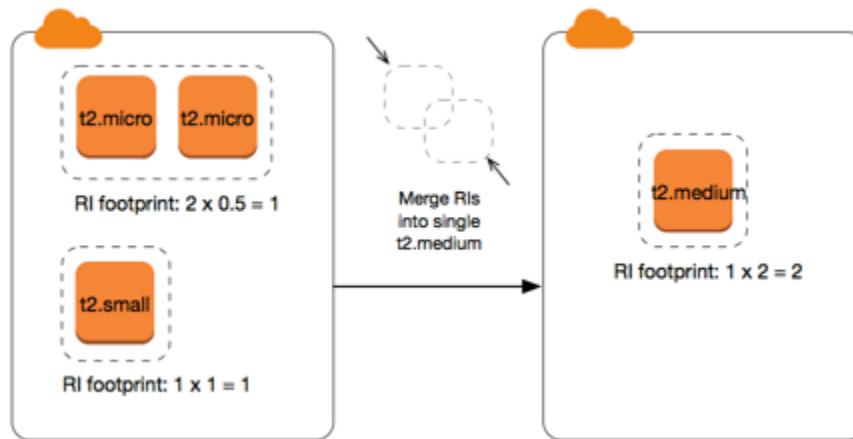
Para calcular o espaço para tamanho de instância de uma Instância reservada, multiplique o número de instâncias pelo fator de normalização. No console do Amazon EC2, o fator de normalização é medido em unidades. A tabela a seguir descreve o fator de normalização para os tamanhos de instância em uma família de instâncias. Por exemplo, `t2.medium` tem um fator de normalização de 2, por isso, uma reserva para quatro instâncias `t2.medium` tem um espaço de 8 unidades.

Tamanho da instância	Fator de normalização
nano	0.25
micro	0,5
small	1
medium	2
large	4
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

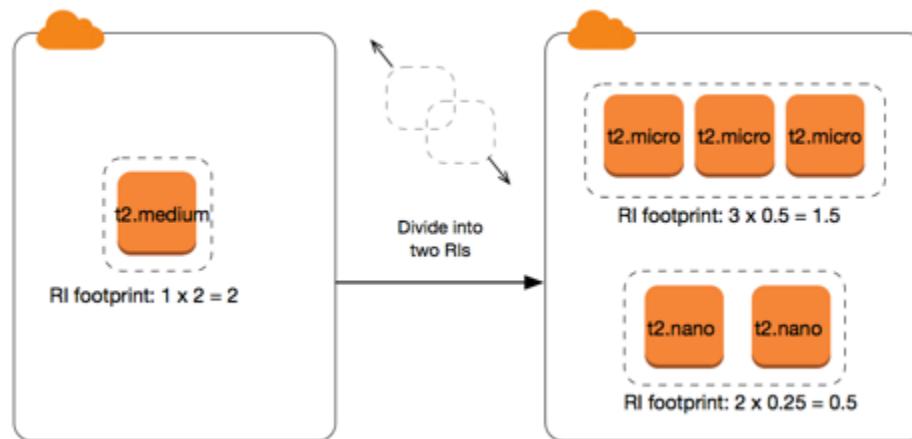
Você pode alocar suas reservas para tamanhos de instância diferentes na mesma família de instâncias, desde que o espaço para o tamanho da instância da sua reserva permaneça o mesmo. Por exemplo, você pode dividir uma reserva para uma instância `t2.large` (1 @ 4 unidades) em quatro instâncias `t2.small` (4 @ 1 unidade). Da mesma forma, você pode combinar uma reserva para quatro instâncias `t2.small` em uma instância `t2.large`. No entanto, você não pode alterar sua reserva para duas instâncias `t2.small` em uma instância `t2.large` porque o espaço da nova reserva (4 unidades) é maior que o espaço da reserva original (2 unidades).

No exemplo a seguir, você tem uma reserva com duas instâncias `t2.micro` (1 unidade) e uma reserva com uma instância `t2.small` (1 unidade). Se você mesclar ambas as reservas em uma única reserva

com uma instância `t2.medium` (2 unidades), o espaço da nova reserva será igual ao espaço das reservas combinadas.



Você também pode modificar uma reserva para dividi-la em duas ou mais reservas. No exemplo a seguir, você tem uma reserva com uma instância `t2.medium` (2 unidades). Você pode dividir a reserva em duas reservas, uma com duas instâncias `t2.nano` (0,5 unidades) e a outra com três instâncias `t2.micro` (1,5 unidades).



#### Fatores de normalização para instâncias bare metal

Você pode modificar uma reserva com instâncias `metal` usando outros tamanhos dentro da mesma família de instâncias. Você pode modificar uma reserva com instâncias diferentes de instâncias bare metal usando o tamanho `metal` dentro da mesma família de instâncias. Geralmente, uma instância bare metal tem o mesmo tamanho que o maior tamanho de instância disponível na mesma família de instâncias. Por exemplo, uma instância `i3.metal` é do mesmo tamanho que uma instância `i3.16xlarge`. Portanto, elas têm o mesmo fator de normalização.

A tabela a seguir descreve o fator de normalização para os tamanhos de instâncias bare metal em famílias de instâncias com instâncias bare metal. O fator de normalização para instâncias `metal` depende da família de instâncias, ao contrário dos outros tamanhos de instância.

Tamanho da instância	Fator de normalização
<code>a1.metal</code>	32

Tamanho da instância	Fator de normalização
m5zn.metal   z1d.metal	96
c6g.metal   c6gd.metal   i3.metal   m6g.metal   m6gd.metal   r6g.metal   r6gd.metal   x2gd.metal	128
c5n.metal	144
c5.metal   c5d.metal   i3en.metal   m5.metal   m5d.metal   m5dn.metal   m5n.metal   r5.metal   r5b.metal   r5d.metal   r5dn.metal   r5n.metal	192
u-* .metal	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, será possível dividir a reserva da seguinte maneira:

- Uma instância `i3.16xlarge` é do mesmo tamanho que uma instância `i3.metal`, portanto, seu fator de normalização é de 128 (128/1). A reserva para uma instância `i3.metal` pode ser modificada para uma instância `i3.16xlarge`.
- Uma instância `i3.8xlarge` tem a metade do tamanho de uma instância `i3.metal`, portanto, seu fator de normalização é de 64 (128/2). A reserva para uma instância `i3.metal` pode ser dividida em duas instâncias `i3.8xlarge`.
- Uma instância `i3.4xlarge` é um quarto do tamanho de uma instância `i3.metal`, portanto, seu fator de normalização é de 32 (128/4). A reserva para uma instância `i3.metal` pode ser dividida em quatro instâncias `i3.4xlarge`.

## Enviar solicitações de modificação

Antes de modificar as instâncias reservadas, leia as [restrições \(p. 376\)](#) aplicáveis. Antes de modificar o tamanho da instância, calcule o [tamanho total ocupado pela instância \(p. 377\)](#) das reservas originais que deseja modificar e assegure-se de que corresponde ao tamanho total ocupado pela instância das novas configurações.

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.
  - Instance Type (Tipo de instância): selecione o tipo de instância necessário. As configurações combinadas devem ser iguais ao tamanho da instância das configurações originais.
  - 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.
  - Instance Type (Tipo de instância): Selecione o tipo de instância necessário. As configurações combinadas devem ser iguais ao tamanho da instância das configurações originais.
  - 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. 376) 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 \(p. 375\)](#).

### Tópicos

- [Requisitos para trocar de Instâncias reservadas conversíveis \(p. 383\)](#)
- [Calcular trocas de Instâncias reservadas conversíveis \(p. 384\)](#)
- [Mesclar Instâncias reservadas conversíveis \(p. 385\)](#)
- [Trocá uma parte de uma Instância reservada convertível \(p. 385\)](#)
- [Enviar solicitações de troca \(p. 386\)](#)

## 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 \(p. 385\)](#). Para obter mais informações sobre como modificar Instâncias reservadas, consulte [Modificar a Instâncias reservadas \(p. 375\)](#).
- 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 \(p. 385\)](#).
- 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:

$3.5 = 3 \text{ whole Convertible Reserved Instances} + 1 \text{ additional Convertible Reserved Instance}$

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.

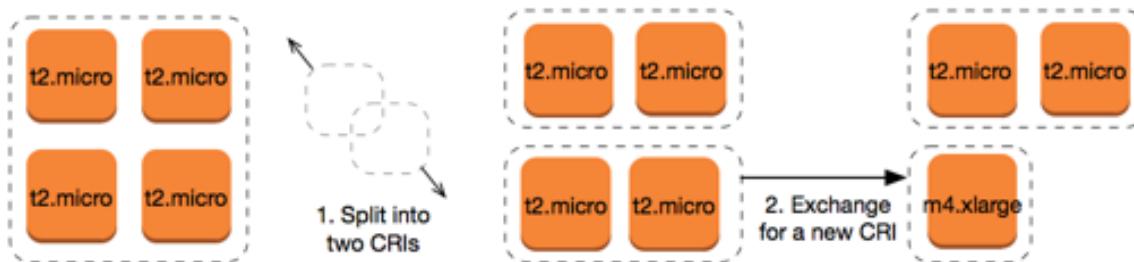
## Trocá uma parte de uma Instância reservada convertível

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`:

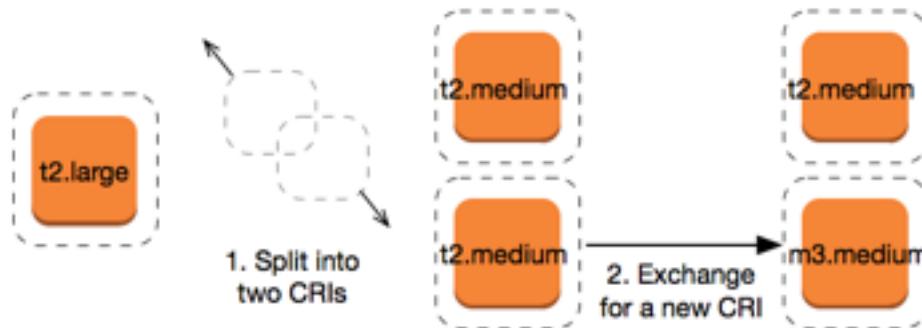
1. Modifique a `t2.micro` Instância reservada convertível dividindo-a em duas `t2.micro` Instâncias reservadas conversíveis com duas instâncias cada uma.
2. Troque uma das novas `t2.micro` Instâncias reservadas conversíveis por uma `m4.xlarge` Instância reservada convertível.



#### Example Exemplo: Instância reservada convertível com uma única instância

Neste exemplo, você tem uma t2.large Instância reservada convertível. Para transformá-la em duas t2.medium Instâncias reservadas conversíveis. Uma única instância t2.large tem o mesmo espaço para tamanho da instância que duas instâncias t2.medium.

1. Modifique a t2.large Instância reservada convertível dividindo-a em duas t2.medium Instâncias reservadas conversíveis. Uma única instância t2.large tem o mesmo espaço para tamanho da instância que duas instâncias t2.medium.
2. Troque uma das novas t2.medium Instâncias reservadas conversíveis por uma m3.medium Instância reservada convertível.



Para obter mais informações, consulte [Suporte para modificar tamanhos de instância \(p. 377\)](#) e [Enviar solicitações de troca \(p. 386\)](#).

#### 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.

#### Trocar 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 \(p. 481\)](#), 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 \(p. 389\)](#)
- [Como começar a usar \(p. 390\)](#)
- [Serviços relacionados \(p. 391\)](#)
- [Definição de preço e economia \(p. 391\)](#)

## 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.

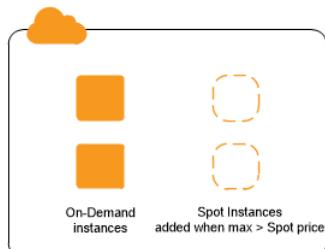
## Principais diferenças entre Instâncias spot e Instâncias on-demand

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 <a href="#">interromper</a> (p. 427) 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. \(p. 5\)](#)
- [Tutorial: Comece a usar instâncias Linux do Amazon EC2 \(p. 9\)](#)

## Noções básicas do spot

- [Como as Instâncias spot funcionam \(p. 394\)](#)

## Trabalho com Instâncias spot

- [Preparar-se para interrupções \(p. 431\)](#)
- [Criar uma solicitação de instância spot \(p. 403\)](#)
- [Obter informações do status da solicitação \(p. 421\)](#)

## 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 \(p. 435\)](#).

## 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 \(p. 396\)](#).

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 \(p. 397\)](#).

## 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 \(p. 393\)](#)
- [Ser flexível sobre tipos de instância e zonas de disponibilidade \(p. 393\)](#)
- [Usar grupos do EC2 Auto Scaling ou frota spot para gerenciar a capacidade agregada \(p. 394\)](#)
- [Usar a estratégia de alocação otimizada por capacidade \(p. 394\)](#)
- [Usar rebalanceamento proativo de capacidade \(p. 394\)](#)
- [Usar produtos integrados da AWS para gerenciar as instâncias spot \(p. 394\)](#)

### 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 \(p. 394\)](#).

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 \(p. 424\)](#). 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 \(p. 423\)](#) e [Interrupções de instâncias spot \(p. 427\)](#).

### 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 \(p. 764\)](#) 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 \(p. 752\)](#) 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 \(p. 753\)](#).

## 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 \(p. 403\)](#).
- 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 \(p. 739\)](#).
- 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 \(p. 764\)](#).

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 \(p. 427\)](#).

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 \(p. 395\)](#)
- [Executar Instâncias spot em um grupo de zonas de disponibilidade \(p. 396\)](#)
- [Executar Instâncias spot em uma VPC \(p. 396\)](#)

## 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.

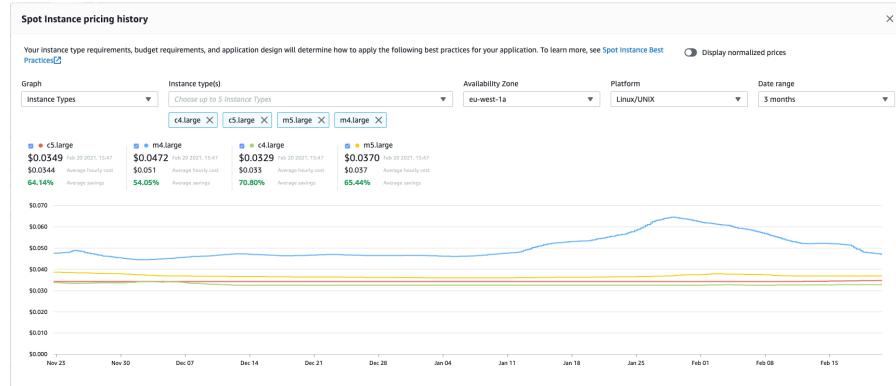
Para exibir os preços spot atuais

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.

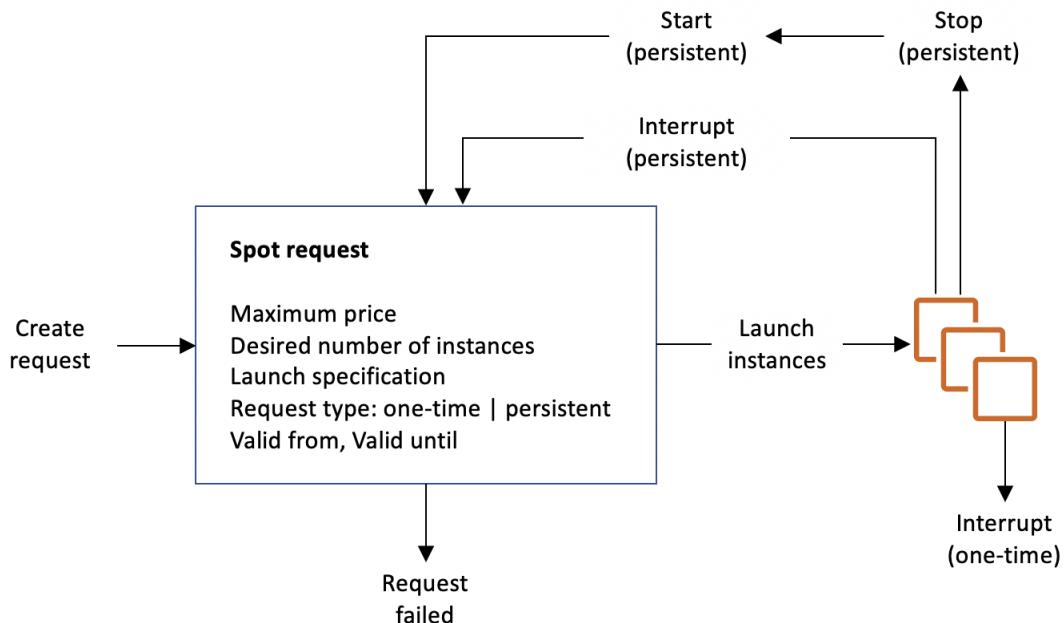
Para visualizar as informações de economias de todas as Instâncias spot em execução (console)

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 \(p. 400\)](#)
- [Definir uma duração para suas Instâncias spot \(p. 401\)](#)
- [Especificar uma locação para suas Instâncias spot \(p. 401\)](#)
- [Função vinculada ao serviço para solicitações de instâncias spot \(p. 401\)](#)

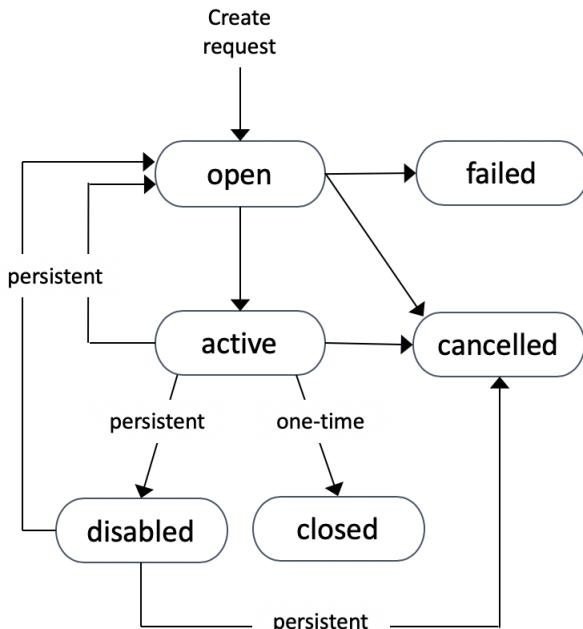
- [Criar uma solicitação de instância spot \(p. 403\)](#)
- [Encontrar Instâncias spot em execução \(p. 406\)](#)
- [Marcar solicitações de instância spot \(p. 407\)](#)
- [Cancelar uma solicitação de instância spot \(p. 412\)](#)
- [Interromper uma instância spot \(p. 412\)](#)
- [Iniciar uma instância spot \(p. 413\)](#)
- [Encerrar uma instância spot \(p. 414\)](#)
- [Exemplo de especificações de execução de solicitações de instância spot \(p. 415\)](#)

## 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 \(p. 412\)](#), [Iniciar uma instância spot \(p. 413\)](#) e [Encerrar uma instância spot \(p. 414\)](#).

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 \(p. 417\)](#).

## 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 \(p. 475\)](#) 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 \(p. 403\)](#).
- 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 \(p. 478\)](#). 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 \(p. 163\)](#) ou um [snapshot do Amazon EBS criptografado \(p. 1418\)](#) 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 \(console\) \(p. 403\)](#).
- 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 \(p. 417\)](#).

Para executar uma frota que inclui Instâncias spot e Instâncias on-demand, consulte [Criar uma solicitação de frota spot \(p. 764\)](#).

### 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 \(p. 396\)](#).

#### 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 \(AMI\) \(p. 511\)](#).
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 \(p. 512\)](#).

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 da aplicação, 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 \(p. 428\)](#).
- (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 \(p. 512\)](#).

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 \(p. 515\)](#).
8. Na página Add Tags (Adicionar tags), especifique as [tags \(p. 1552\)](#) fornecendo combinações de chave e valor. Para obter mais informações, consulte [Etapa 5: Adicionar tags \(p. 516\)](#).
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 Linux \(p. 1225\)](#).) Selecione ou crie um grupo de segurança e escolha Revisar e executar. Para obter mais informações, consulte [Etapa 6: configurar o grupo de segurança \(p. 516\)](#).
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 \(p. 517\)](#).
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 Linux \(p. 1209\)](#).

**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 \(p. 1568\)](#).

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 \(p. 415\)](#). 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 \(p. 1552\)](#).

### Tópicos

- [Prerequisites \(p. 407\)](#)
- [Marcar uma nova solicitação de instância spot \(p. 409\)](#)
- [Marcar uma solicitação de instância spot existente \(p. 410\)](#)
- [Exibir tags de solicitação de instância spot \(p. 410\)](#)

## 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 \(p. 403\)](#).
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 \(p. 403\)](#).

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 \(p. 1559\)](#).

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 \(p. 414\)](#).

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 \(p. 412\)](#).

## 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 \(p. 403\)](#).

1. Executar Instâncias spot (p. 415)
2. Executar Instâncias spot na zona de disponibilidade especificada (p. 416)
3. Executar Instâncias spot na sub-rede especificada (p. 416)
4. Executar uma instância spot dedicada (p. 417)

### 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.

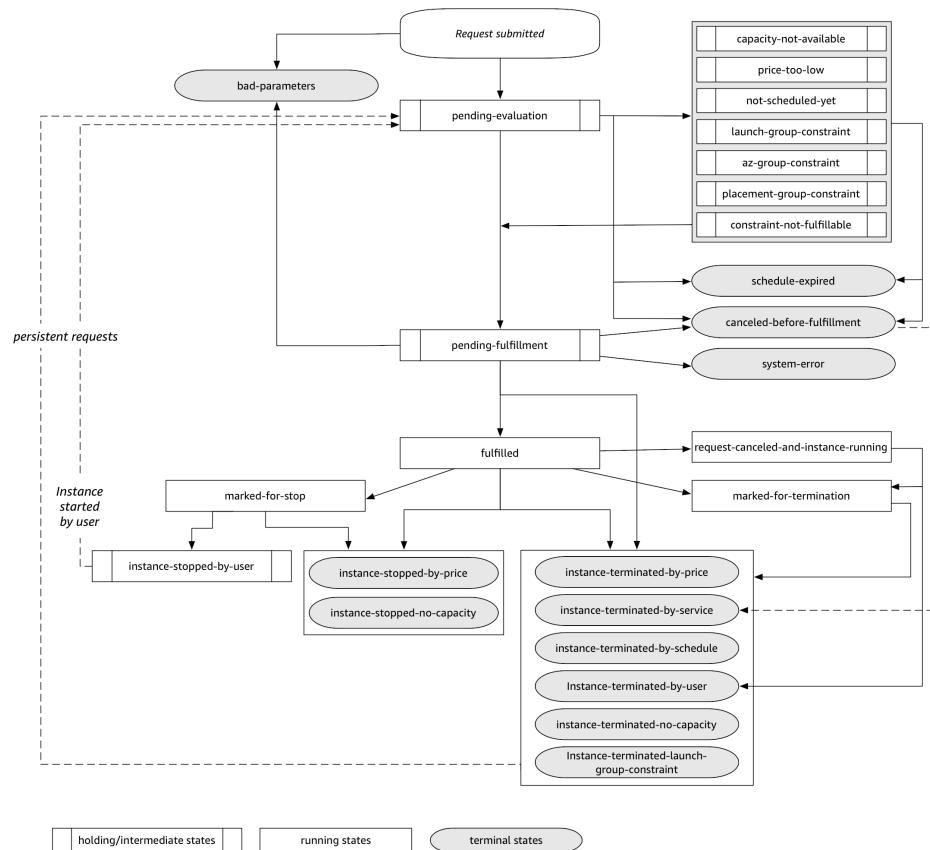
Em cada etapa do processo — também denominado ciclo de vida da solicitação spot — eventos específicos determinam estados sucessivos de solicitação.

### Tópicos

- [Ciclo de vida de uma solicitação spot \(p. 417\)](#)
- [Obter informações do status da solicitação \(p. 421\)](#)
- [Códigos de status das solicitações spot \(p. 421\)](#)

## 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
<b>pending-evaluation</b>	<b>open</b>	n/a
<b>bad-parameters</b>	<b>closed</b>	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>	active	stopping
<code>instance-stopped-by-user</code> *	disabled ou cancelled**	stopped

\* 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 (única), open (persistente)</code>	<code>terminated</code>

Código de status	Estado da solicitação	Estado da instância
instance-terminated-by-schedule	closed	terminated
instance-terminated-by-service	cancelled	terminated
instance-terminated-by-user	closed ou cancelled *	terminated
instance-terminated-no-capacity	closed (única), open (persistente)	terminated
instance-terminated-launch-group-constraint	closed (única), open (persistente)	terminated

\* 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 \(p. 432\)](#), 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 \(p. 424\)](#)
- [Monitorar os sinais de recomendação de rebalanceamento \(p. 424\)](#)
- [Serviços que usam o sinal de recomendação de rebalanceamento \(p. 427\)](#)

## 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 \(p. 725\)](#) para EC2 Fleet e [Rebalanceamento de capacidade \(p. 753\)](#) 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 \(p. 424\)](#)
- [Usar metadados da instância \(p. 426\)](#)

## 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.

#### 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/recommendations/rebalance
```

#### IMDSv1

```
[ec2-user ~]$ curl 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 \(p. 725\)](#) no tópico Frota do EC2 deste guia do usuário
- [Rebalanceamento de capacidade \(p. 753\)](#) 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 \(p. 427\)](#)
- [Comportamentos de interrupção \(p. 428\)](#)
- [Especificar o comportamento de interrupção \(p. 430\)](#)
- [Preparar-se para interrupções \(p. 431\)](#)
- [Preparar a hibernação de uma instância \(p. 431\)](#)
- [Avisos de interrupção de instância spot \(p. 432\)](#)
- [Encontrar Instâncias spot interrompidas \(p. 434\)](#)
- [Determinar se o Amazon EC2 interrompeu uma instância spot \(p. 434\)](#)
- [Faturamento para Instâncias spot interrompidas \(p. 435\)](#)

## 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 \(p. 428\)](#)
- [Hibernar Instâncias spot interrompida \(p. 429\)](#)
- Encerre Instâncias spot interrompidas (este é o comportamento padrão)

Para alterar o comportamento de interrupção, consulte [Especificar o comportamento de interrupção \(p. 430\)](#).

### 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 \(p. 163\)](#).
- 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 \(p. 1421\)](#).
- 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 \(p. 167\)](#) e [Copiar um AMI \(p. 145\)](#).

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 coloca 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 \(p. 431\)](#).

Para obter informações sobre a hibernação de Instâncias on-demand, consulte [Hibernar a instância do Windows sob demanda ou reservada \(p. 566\)](#).

### 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 \(p. 510\)](#), 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 \(p. 764\)](#), 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 \(p. 519\)](#), 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 \(p. 423\)](#).
- 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 \(p. 432\)](#).
- 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.

Os procedimentos a seguir ajudam você a preparar uma instância do Linux. Para obter instruções sobre como preparar uma instância Windows, consulte [Preparar para hibernação de uma instância](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

### Para preparar uma instância do Amazon Linux

1. Verifique se o kernel oferece suporte à hibernação e atualize-o, se necessário.
2. Se sua AMI não incluir o agente, instale-o usando o seguinte comando:

```
sudo yum update; sudo yum install hibagent
```

3. Adicione o seguinte aos dados do usuário:

```
#!/bin/bash  
/usr/bin/enable-ec2-spot-hibernation
```

Para preparar uma instância do Ubuntu

1. Se sua AMI não incluir o agente, instale-o usando o seguinte comando: O agente de hibernação só está disponível no Ubuntu 16.04 ou posterior.

```
sudo apt-get install hibagent
```

2. Adicione o seguinte aos dados do usuário:

```
#!/bin/bash  
/usr/bin/enable-ec2-spot-hibernation
```

## 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 \(p. 649\)](#) 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 \(p. 649\)](#). Caso contrário, não estará presente. Você pode recuperar `instance-action` da maneira a seguir.

#### 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/spot/instance-action
```

#### IMDSv1

```
[ec2-user ~]$ curl 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.

#### IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
[ec2-user ~]$ if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo terminated; fi
```

#### IMDSv1

```
[ec2-user ~]$ if curl -s http://169.254.169.254/latest/meta-data/spot/termination-time \
| grep -q .*T.*Z; then echo terminated; fi
```

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 encerra 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 \(p. 919\)](#).

## 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 \(p. 436\)](#)
- [Requisitos do bucket do Amazon S3 \(p. 436\)](#)
- [Assinar seu feed de dados da instância spot \(p. 437\)](#)
- [Descrever seu feed de dados de instância spot \(p. 437\)](#)
- [Excluir seu feed de dados de instância spot \(p. 438\)](#)

## 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 \(p. 438\)](#)
- [Solicitar um aumento de limite de instância spot \(p. 439\)](#)

## 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 \(p. 1565\)](#) 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 \(p. 1565\)](#).

## Instâncias expansíveis

Se você executar as Instâncias spot usando um [tipo de instância de performance intermitente \(p. 228\)](#) 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 \(p. 245\)](#) para evitar pagar custos mais elevados. Se executar as instâncias spot expansíveis no [modo ilimitado \(p. 237\)](#) 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 \(p. 239\)](#).

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. 237) 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 \(p. 440\)](#)
- [Traga sua própria licença \(p. 441\)](#)
- [Capacidade da instância do Host dedicado \(p. 441\)](#)
- [Instâncias T3 intermitentes em hosts dedicados \(p. 442\)](#)
- [Restrições do Hosts dedicados \(p. 443\)](#)
- [Definição de preço e faturamento \(p. 444\)](#)
- [Como trabalhar com o Hosts dedicados \(p. 445\)](#)
- [Trabalhar com Hosts dedicados compartilhado \(p. 464\)](#)
- [Recuperação do host \(p. 469\)](#)
- [Monitorar alterações de configuração \(p. 473\)](#)

## 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 <a href="#">Recuperação do host (p. 469)</a> .	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.
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.

### 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 \(p. 473\)](#).

## 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"><li>Exemplo 1: 4 x r5.4xlarge + 4 x r5.2xlarge</li><li>Exemplo 2: 1 x r5.12xlarge + 1 x r5.4xlarge + 1 x r5.2xlarge + 5 x r5.xlarge + 2 x r5.large</li></ul>
C5	<ul style="list-style-type: none"><li>Exemplo 1: 1 x c5.9xlarge + 2 x c5.4xlarge + 1 x c5.xlarge</li><li>Exemplo 2: 4 x c5.4xlarge + 1 x c5.xlarge + 2 x c5.large</li></ul>
M5	<ul style="list-style-type: none"><li>Exemplo 1: 4 x m5.4xlarge + 4 x m5.2xlarge</li><li>Exemplo 2: 1 x m5.12xlarge + 1 x m5.4xlarge + 1 x m5.2xlarge + 5 x m5.xlarge + 2 x m5.large</li></ul>

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 \(p. 245\)](#).

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 \(p. 880\)](#).

## 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 \(p. 441\)](#).

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 \(p. 444\)](#)
- [Dedicated Host Reservations \(p. 444\)](#)
- [Savings Plans \(p. 445\)](#)
- [Definição de preço para o Windows Server no Hosts dedicados \(p. 445\)](#)

## 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 \(p. 460\)](#).

## 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 \(p. 204\)](#). 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 \(p. 446\)](#)
- [Execute instâncias em um Host dedicado. \(p. 448\)](#)
- [Execute instâncias em um grupo de recursos de host. \(p. 450\)](#)
- [Noções básicas sobre posicionamento automático e afinidade \(p. 451\)](#)
- [Modificar posicionamento automático de Host dedicado \(p. 452\)](#)
- [Modificar os tipos de instância compatíveis \(p. 453\)](#)
- [Modificar locação e da afinidade de instâncias \(p. 455\)](#)
- [Visualização do Hosts dedicados \(p. 456\)](#)

- [Marcação de Hosts dedicados \(p. 458\)](#)
- [Monitorar Hosts dedicados \(p. 459\)](#)
- [Liberar Hosts dedicados \(p. 460\)](#)
- [Comprar Reservas de hosts dedicados \(p. 461\)](#)
- [Visualizar reservas de Host dedicado \(p. 463\)](#)
- [Atribuir tag de Reservas de hosts dedicados \(p. 463\)](#)

## 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`, e `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 \(p. 451\)](#).

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 \(p. 469\)](#).
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 \(p. 451\)](#).
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 \(p. 469\)](#).
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 \(p. 443\)](#).

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 \(p. 451\)](#).

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 \(p. 451\)](#).

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 alocará 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 o 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 \(p. 451\)](#).
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 \(p. 451\)](#).

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 \(p. 475\)](#).
  - 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 \(p. 451\)](#).

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.

```
$ 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 \(p. 446\)](#).

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
<code>available</code>	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 <a href="#">modificado para oferecer suporte a vários tipos de instância (p. 453)</a> , ou uma <a href="#">recuperação de host (p. 469)</a> 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 \(p. 465\)](#)
- [Limitações para compartilhamento de Host dedicado \(p. 465\)](#)
- [Serviços relacionados \(p. 465\)](#)
- [Compartilhamento entre zonas de disponibilidade \(p. 465\)](#)
- [Compartilhar um Host dedicado \(p. 465\)](#)
- [Descompartilhar um Host dedicado compartilhado \(p. 466\)](#)
- [Identificar um Host dedicado compartilhado \(p. 467\)](#)
- [Visualizar instâncias em execução em um Host dedicado compartilhado \(p. 468\)](#)
- [Permissões de Host dedicado compartilhado \(p. 468\)](#)
- [Faturamento e medição \(p. 468\)](#)
- [Limites de Host dedicado \(p. 469\)](#)
- [Recuperação de host e compartilhamento do Host dedicado \(p. 469\)](#)

## 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 [Creating a Resource Share \(Criar um compartilhamento de recursos\)](#) no AWS RAM User Guide (Guia 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

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 do qual cancelar o compartilhamento e escolha a guia Compartilhamento.
4. 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

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. 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 \(p. 469\)](#).

## 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 \(p. 469\)](#)
- [Tipos de instâncias compatíveis \(p. 470\)](#)
- [Configurar a recuperação do host \(p. 471\)](#)
- [Estados de recuperação do host \(p. 472\)](#)
- [Recuperar manualmente instâncias incompatíveis \(p. 472\)](#)
- [Serviços relacionados \(p. 473\)](#)
- [Pricing \(p. 473\)](#)

## 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 a 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, C6g, Inf1, M3, M4, M5, M5n, M6g, P3, R3, R4, R5, R5n, R6g, X1, X1e, X2gd, u-6tb1, u-9tb1, u-12tb1, u-18tb1 e u-24tb1.

Para recuperar instâncias não compatíveis, consulte [Recuperar manualmente instâncias incompatíveis \(p. 472\)](#).

## 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 \(p. 471\)](#)
- [Desativar a recuperação do host \(p. 471\)](#)
- [Visualizar a configuração de recuperação do host \(p. 471\)](#)

### 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 \(p. 446\)](#).

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 \(p. 562\)](#).

### 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 \(p. 440\)](#).

### Tópicos

- [Conceitos básicos da Instâncias dedicadas \(p. 475\)](#)
- [Recursos compatíveis \(p. 476\)](#)
- [Diferenças entre instâncias dedicadas e hosts dedicados \(p. 477\)](#)
- [Limitações da Instâncias dedicadas \(p. 477\)](#)
- [Definição de preço para Instâncias dedicadas \(p. 478\)](#)
- [Como trabalhar com Instâncias dedicadas \(p. 478\)](#)

## 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 \(p. 440\)](#).

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 \(p. 478\)](#).

- 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 \(p. 479\)](#).

## Recursos compatíveis

Instâncias dedicadas são compatíveis com os seguintes recursos e integrações de serviço da AWS:

### Tópicos

- [Reserved Instances \(p. 476\)](#)
- [Escalabilidade automática \(p. 476\)](#)
- [Recuperação automática \(p. 476\)](#)
- [Instâncias spot dedicadas \(p. 476\)](#)
- [Instâncias expansíveis \(p. 476\)](#)

### 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 \(p. 343\)](#).

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 \(p. 593\)](#).

### 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 [Especificar uma locação para suas Instâncias spot \(p. 401\)](#).

### Instâncias expansíveis

É possível aproveitar os benefícios da execução em hardware de locação dedicada com [the section called "Instâncias expansíveis" \(p. 228\)](#). 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” \(p. 230\)](#).

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 servidor 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 \(p. 440\)](#).

## 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 \(p. 478\)](#)
- [Executar Instâncias dedicadas em um VPC \(p. 479\)](#)
- [Exibir informações de locação \(p. 479\)](#)
- [Altere a locação de uma instância \(p. 480\)](#)
- [Alterar a locação de uma VPC \(p. 481\)](#)

## 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. \(p. 448\)](#).

### 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 \(p. 485\)](#).

#### Tópicos

- [Diferenças entre Reservas de Capacidade, Instâncias reservadas e Savings Plans \(p. 482\)](#)
- [Plataformas compatíveis \(p. 483\)](#)
- [Limites da Reserva de capacidade \(p. 484\)](#)
- [Restrições e limitações de Reserva de capacidade \(p. 484\)](#)
- [Definição de preços e faturamento da Reserva de capacidade \(p. 484\)](#)
- [Como trabalhar com Reservas de Capacidade \(p. 485\)](#)
- [Reservas de Capacidade em Local Zones \(p. 495\)](#)
- [Reservas de Capacidade em zonas Wavelength \(p. 496\)](#)
- [Reservas de Capacidade no AWS Outposts \(p. 496\)](#)
- [Como trabalhar com Reservas de Capacidade compartilhadas \(p. 497\)](#)
- [Métricas do CloudWatch para Reservas de Capacidade sob demanda \(p. 502\)](#)

## 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	Exige compromisso fixo de um ano ou de três anos		

	Capacity Reservations	Instâncias reservadas zonais	Instâncias reservadas regionais	Savings Plans	
	ser criadas e canceladas conforme necessário.				
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 pode solicitar um aumento de limite.	O padrão é 20 por região. Você pode solicitar um aumento de limite.	Sem 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 \(p. 343\)](#)
- [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:

- Linux/UNIX
- Linux com SQL Server Standard
- Linux com SQL Server Web
- Linux com SQL Server Enterprise
- Red Hat Enterprise Linux
- SUSE Linux

Quando adquire uma Reserva de capacidade, você deve escolher uma oferta para uma plataforma que represente o sistema operacional da sua instância.

- Para distribuições SUSE Linux e RHEL, excluindo BYOL, você deve escolher a plataforma específica. Por exemplo, a plataforma SUSE Linux ou Red Hat Enterprise Linux .
- Para todas as demais distribuições do Linux (incluindo Ubuntu), escolha uma oferta para a plataforma Linux/UNIX.
- Se você trouxer sua assinatura RHEL (BYOL) existente, deve escolher a plataforma Linux/UNIX .

Para obter mais informações sobre as plataformas Windows compatíveis, consulte [Plataformas compatíveis](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## 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 \(p. 497\)](#).
- 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.
- 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 \(p. 485\)](#).

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

demandas 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 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	4	5	6
<b>Unused Capacity Reservation</b>	\$0.10	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
<b>On-demand Instance Usage</b>	\$0.00	\$0.10	\$0.10	\$0.10	\$0.10	\$0.10
<b>Hourly cost</b>	<b>\$0.10</b>	<b>\$0.10</b>	<b>\$0.10</b>	<b>\$0.10</b>	<b>\$0.10</b>	<b>\$0.10</b>

## 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 \(p. 343\)](#)
- [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 \(p. 486\)](#)
- [Trabalhar com grupos de Reserva de capacidade \(p. 487\)](#)
- [Iniciar instâncias em uma Reserva de capacidade existente \(p. 491\)](#)
- [Modifique uma Reserva de capacidade \(p. 492\)](#)
- [Modificar as configurações da Reserva de capacidade de uma instância \(p. 493\)](#)
- [Visualizar uma Reserva de capacidade \(p. 494\)](#)
- [Cancelar uma Reserva de capacidade \(p. 494\)](#)

## 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 \(p. 340\)](#).

### 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 \(p. 1248\)](#).
  - 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 \(p. 483\)](#). Para obter mais informações sobre as plataformas Windows compatíveis, consulte [Plataformas compatíveis](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.
  - 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 excede 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 \(p. 483\)](#). Para obter mais informações sobre as plataformas Windows compatíveis, consulte [Plataformas compatíveis](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Por exemplo, o comando a seguir cria uma Reserva de capacidade que reserva capacidade para três instâncias `m5.2xlarge`, executando AMIs do Red Hat Enterprise Linux na zona de disponibilidade `us-east-1a`.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-platform Red Hat Enterprise Linux --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.

```
$ 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`.

```
$ 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`.

```
$ aws resource-groups list-group-resources --group MyCRGroup
```

Veja a seguir um exemplo de saída.

```
{  
    "QueryErrors": [],  
    "ResourceIdentifiers": [  
        {  
            "ResourceType": "AWS::EC2::CapacityReservation",  
            "ResourceIdentifier": "cr-1234567890abcdef1"  
        }  
    ]  
}
```

```
        "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.

```
$ 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.

```
$ 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`.

```
$ 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 excede 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
- Impreça 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 \(p. 493\)](#).

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 \(p. 486\)](#).
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 \(p. 491\)](#).

## 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 \(p. 486\)](#).
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 \(p. 491\)](#).

## 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 \(p. 497\)](#).

#### 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 \(p. 486\)](#).

#### 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 compartilharam. 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 \(p. 498\)](#)
- [Serviços relacionados \(p. 498\)](#)
- [Compartilhamento entre zonas de disponibilidade \(p. 498\)](#)
- [Compartilhar uma Reserva de capacidade \(p. 499\)](#)
- [Parar de compartilhar uma Reserva de capacidade \(p. 500\)](#)
- [Identificar uma Reserva de capacidade compartilhada \(p. 500\)](#)
- [Exibir uso de Reserva de capacidade compartilhado \(p. 501\)](#)
- [Permissões de Reserva de capacidade compartilhada \(p. 501\)](#)
- [Faturamento e medição \(p. 501\)](#)
- [Limites de instâncias \(p. 502\)](#)

## 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 \(p. 502\)](#)
- [Dimensões de métricas da Reserva de capacidade \(p. 503\)](#)
- [Visualizar métricas do CloudWatch nas Reservas de Capacidade \(p. 503\)](#)

## 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

Métrica	Descrição
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)

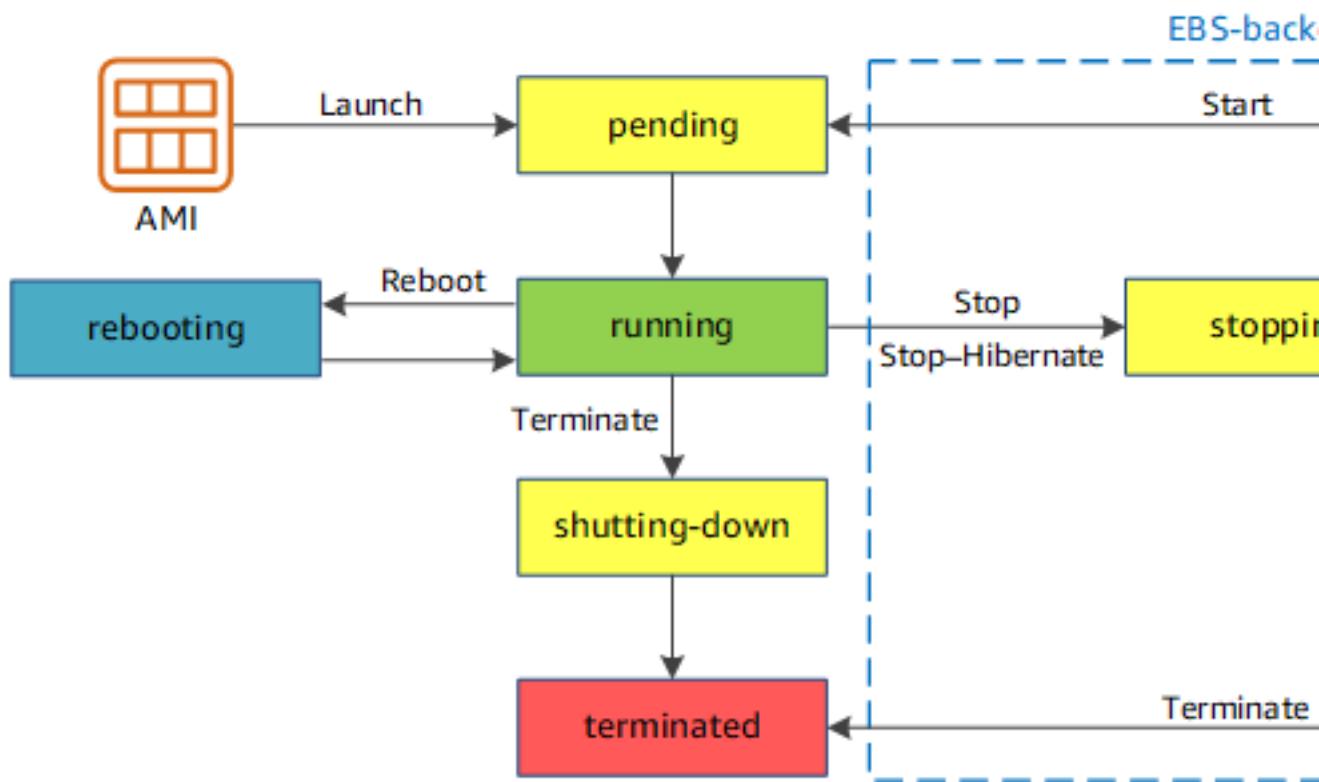
Use o comando [list-metrics](#) a seguir:

```
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. Observe que você não pode parar e o iniciar uma instância com armazenamento de instâncias. Para obter mais informações sobre instâncias baseadas em armazenamento de instâncias, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#).



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
<b>pending</b>	A instância está se preparando para entrar no estado <b>running</b> . Uma instância entra no estado <b>pending</b> quando ela é executada pela primeira vez ou quando é iniciada após estar no estado <b>stopped</b> .	Não faturado
<b>running</b>	A instância está em execução e pronta para uso.	Faturado
<b>stopping</b>	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

Estado da instância	Descrição	Faturamento para uso da instância
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	A 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 <a href="#">Reserved Instances (p. 343)</a>

#### 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 \(p. 509\)](#) e [Conecte-se à sua instância do Linux \(p. 535\)](#).

## 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 \(p. 562\)](#).

## 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 \(p. 505\)](#) 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 Windows sob demanda ou reservada \(p. 566\)](#).

## Reinicialização da instância

Você pode reiniciar 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 reiniciar 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 um novo período de faturamento de instância; o faturamento por segundo continua sem a cobrança mínima de um minuto.

Para obter mais informações, consulte [Reiniciar a instância \(p. 583\)](#).

## 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 \(p. 584\)](#).

## 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 a instância é parada ou encerrada ao iniciar uma desativação de dentro da instância em si (por exemplo, usando o comando `shutdown` no Linux). 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 \(p. 587\)](#).

## 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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Diferenças entre reinicialização,  
interrupção, hibernação e encerramento

Característica	Reiniciar	Parar/iniciar (somente instâncias com Amazon EBS)	Hibernação (somente instâncias baseadas em Amazon EBS)	Encerrar
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 <code>stopping</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.	Você incorre em cobranças quando a instância está no estado <code>stopping</code> , mas não incorre em 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.	As cobranças de uma instância são interrompidas assim que o 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 \(p. 591\)](#).

## 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.	<a href="#">É possível executar uma instância usando o assistente de execução de instância. (p. 510)</a>
[Console do Amazon EC2] Crie um modelo de execução e execute a instância a partir desse modelo.	<a href="#">Executar uma instância a partir de um modelo de execução (p. 517)</a>
[Console do Amazon EC2] Use uma instância existente como base.	<a href="#">Executar uma instância usando parâmetros de uma instância existente (p. 532)</a>
[Console do Amazon EC2] Use uma AMI comprada do AWS Marketplace .	<a href="#">Executar uma instância AWS Marketplace (p. 533)</a>
[AWS CLI] Use uma AMI selecionada.	<a href="#">Usar o Amazon EC2 pela AWS CLI</a>
[AWS Tools for Windows PowerShell] Use uma AMI selecionada.	<a href="#">Amazon EC2 pela AWS Tools for Windows PowerShell</a>
[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.	<a href="#">EC2 Fleet (p. 700)</a>
[AWS CloudFormation] Use um modelo de AWS CloudFormation para especificar uma instância.	<a href="#">AWS::EC2::Instance</a> no Manual do usuário do AWS CloudFormation
[AWS SDK] Use um SDK específico de idioma da AWS para executar uma instância.	<a href="#">AWS SDK for .NET da AWS</a> <a href="#">AWS SDK para C++</a> <a href="#">AWS SDK para Go</a> <a href="#">AWS SDK para Java</a> <a href="#">AWS SDK para JavaScript</a> <a href="#">AWS SDK para PHP V3</a>

Método	Documentação
	<a href="#">AWS SDK for Python</a>
	<a href="#">AWS SDK para Ruby V3</a>

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 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 \(p. 210\)](#).

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 [Conecte-se à sua instância do Linux \(p. 535\)](#).

Quando você tiver terminado com uma instância, encerre-a. Para obter mais informações, consulte [Encerrar a instância \(p. 587\)](#).

## 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. \(p. 5\)](#).

### 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 \(p. 511\)](#)
- [Etapa 1: Escolher uma imagem de máquina da Amazon \(AMI\) \(p. 511\)](#)
- [Etapa 2: escolher um tipo de instância \(p. 512\)](#)

- [Etapa 3: configurar detalhes da instância \(p. 512\)](#)
- [Etapa 4: adicionar armazenamento \(p. 515\)](#)
- [Etapa 5: Adicionar tags \(p. 516\)](#)
- [Etapa 6: configurar o grupo de segurança \(p. 516\)](#)
- [Etapa 7: Revisar a execução da instância e selecionar o par de chaves \(p. 517\)](#)

## 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 \(p. 1542\)](#).
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, Linux, 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 \(p. 511\)](#) ou [pesquisar por parâmetro do Systems Manager \(p. 512\)](#).

### 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 \(p. 533\)](#).

#### 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 Root device type (Tipo de dispositivo raiz) listado para cada AMI. Observe que as AMIs são tipo de que você precisa, seja ebs (com Amazon EBS) ou instance-store (com armazenamento de instâncias). Para obter mais informações, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#).
3. 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. Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#).
4. 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 \(p. 79\)](#).
5. 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 \(p. 203\)](#).

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 \(p. 228\)](#).

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 \(p. 403\)](#).
- 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 \(p. 938\)](#).
- 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 Linux 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 [Unir perfeitamente uma instância do EC2 do Linux ao diretório do Microsoft AD gerenciado pela AWS](#).
- 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 \(p. 1084\)](#).
- 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 \(p. 491\)](#).

- 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 \(p. 616\)](#).
- 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 \(p. 591\)](#).
- 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 Windows sob demanda ou reservada \(p. 566\)](#).
- 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 \(p. 589\)](#).
- 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 \(p. 872\)](#).
- 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 \(p. 1438\)](#).
- 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 \(p. 475\)](#) e [Dedicated Hosts \(p. 440\)](#).
- 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 \(p. 228\)](#).
- Sistemas de arquivos: Para criar um novo sistema de arquivos para montar na instância, escolha Create new file system (Criar novo sistema de arquivos), insira um nome para o novo sistema de arquivos e escolha Create (Criar). O sistema de arquivos é criado usando Quick Create (Criação rápida) de Amazon EFS, que aplica as configurações recomendadas pelo serviço. Os grupos de segurança necessários para habilitar o acesso ao sistema de arquivos são criados e anexados automaticamente à instância e aos destinos de montagem do sistema de arquivos. Você também pode optar por criar e anexar manualmente os grupos de segurança necessários. Para obter mais informações, consulte [Criar um sistema de arquivos do EFS usando a Criação rápida do Amazon EFS \(p. 1516\)](#).

Para montar um ou mais sistemas de arquivos de Amazon EFS existentes na instância, escolha Add file system (Adicionar sistema de arquivos) e, em seguida, escolha os sistemas de arquivos a serem montados e os pontos de montagem a serem usados. Para obter mais informações, consulte [Criar um sistema de arquivos de EFS e montá-lo na sua instância \(p. 1517\)](#).

- 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 \(p. 984\)](#). 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 \(p. 942\)](#).

- 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 \(p. 650\)](#).
- 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 \(p. 657\)](#).
- 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 \(p. 654\)](#).
- 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 \(p. 650\)](#).
- 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 \(p. 1494\)](#) e [Volumes do Amazon EBS \(p. 1250\)](#).
- 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 \(p. 1271\)](#).
- 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 \(p. 1253\)](#).
- 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 \(p. 591\)](#).
- 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 \(p. 1418\)](#).

## Etapa 5: Adicionar tags

Na página Add Tags (Adicionar tags), especifique as [tags \(p. 1552\)](#) 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 Linux \(p. 1225\)](#).) 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 SSH (porta 22).
- 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 Linux \(p. 1209\)](#).

### 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 \(p. 846\)](#).

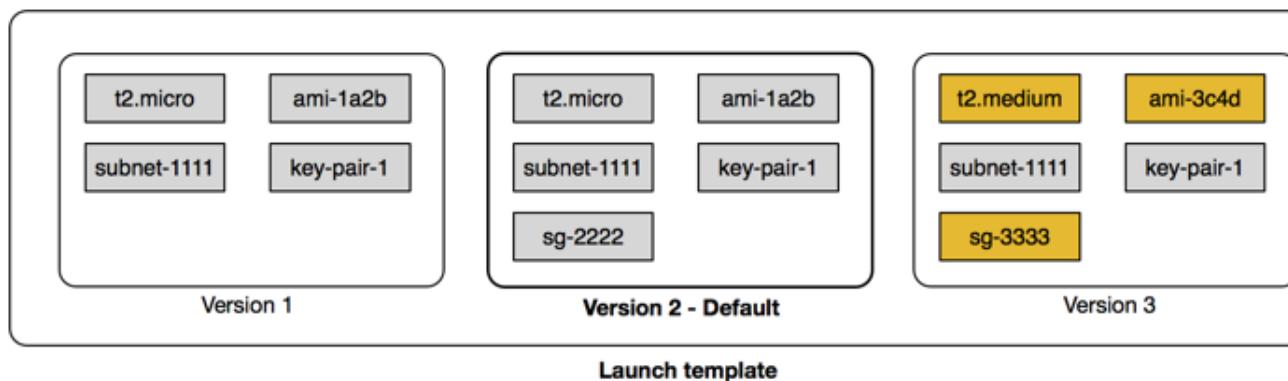
Se a instância não executar ou o estado passar imediatamente para terminated, em vez de running, consulte [Solucionar problemas de execução de instâncias \(p. 1568\)](#).

## 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 \(p. 518\)](#)
- [Uso de modelos de execução para controlar parâmetros de execução \(p. 519\)](#)
- [Controlar o uso dos modelos de execução \(p. 519\)](#)
- [Criar um modelo de execução \(p. 519\)](#)
- [Modificar um modelo de inicialização \(gerenciar versões do modelo de inicialização\) \(p. 526\)](#)
- [Executar uma instância a partir de um modelo de execução \(p. 529\)](#)
- [Usar modelos de execução com o Amazon EC2 Auto Scaling \(p. 530\)](#)
- [Usar modelos de execução com o Frota do EC2 \(p. 531\)](#)
- [Usar modelos de execução com a frota spot \(p. 531\)](#)
- [Excluir um modelo de execução \(p. 531\)](#)

## 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 \(p. 519\)](#)
- [Criar um modelo de execução a partir de um modelo de execução existente \(p. 524\)](#)
- [Criar um modelo de execução a partir de uma instância \(p. 524\)](#)

### 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 \(p. 203\)](#).
  - 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 Linux \(p. 1209\)](#).
  - 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 Linux \(p. 1225\)](#).
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 \(p. 1494\)](#) e [Volumes do Amazon EBS \(p. 1250\)](#).
  - 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 \(p. 1253\)](#).
  - 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 \(p. 591\)](#).
  - 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 \(p. 1418\)](#).
  - 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 \(p. 1552\)](#) 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 \(p. 984\)](#) 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.
  - Elastic Fabric Adapter: indica se a interface de rede é um Elastic Fabric Adapter. Para obter mais informações, consulte [Elastic Fabric Adapter](#).
  - 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 \(p. 389\)](#).
  - 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 \(p. 591\)](#).
  - 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 Windows sob demanda ou reservada \(p. 566\)](#).

- Termination protection (Proteção contra encerramento): se encerramento acidental deve ser impedido. Para obter mais informações, consulte [Habilitar a proteção contra encerramento \(p. 589\)](#).
- 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 \(p. 872\)](#).
- 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 \(p. 228\)](#).
- 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 \(p. 1084\)](#).
- 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 \(p. 1438\)](#).
- 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 \(p. 491\)](#).
- 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 \(p. 475\)](#) e [Dedicated Hosts \(p. 440\)](#).
- 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 \(p. 650\)](#).
- 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 \(p. 654\)](#).
- 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 \(p. 650\)](#).

- 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 Linux na inicialização \(p. 642\)](#).

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 \(p. 519\)](#).

## 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 \(p. 526\)](#)
- [Definir a versão do modelo de execução padrão \(p. 527\)](#)
- [Descrever uma versão de modelo de execução \(p. 527\)](#)
- [Excluir uma versão de modelo de execução \(p. 528\)](#)

### 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 \(p. 519\)](#).

#### 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-0abcd290751193123 \
--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-0abcd290751193123 \
```

--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 \(p. 1568\)](#).

## 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. \(p. 739\)](#).

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 \(p. 749\)](#).

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 \(p. 517\)](#) 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 \(p. 938\)](#).
- 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

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 \(p. 1568\)](#).

#### 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 \(p. 1568\)](#).

## 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 \(p. 102\)](#). 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 \(p. 106\)](#).

##### 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. \(p. 510\)](#). 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 [Conecte-se à sua instância do Linux \(p. 535\)](#).

#### 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 \(p. 106\)](#).

10. Se a instância não executar ou o estado passar imediatamente para `terminated`, em vez de `running`, consulte [Soluçaoar problemas de execução de instâncias \(p. 1568\)](#).

## 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 <code>run-instances</code> ou consulte o tópico a seguir para obter mais informações: <a href="#">Execução de uma instância</a> .

Método	Documentação
AWS Tools for Windows PowerShell	Use o comando <a href="#">New-EC2Instance</a> ou consulte o tópico a seguir para obter mais informações: <a href="#">Executar uma instância do Amazon EC2 usando o Windows PowerShell</a>
API de consulta	Use a solicitação <a href="#">RunInstances</a> .

## Conecte-se à sua instância do Linux

Conecte-se às instâncias do Linux que você executou e transfira arquivos entre seu computador local e sua instância.

Para se conectar a uma instância do Windows, consulte [Conexão com a instância do Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

### Opções de conexão

O sistema operacional do computador local determina as opções que você precisa conectar do computador local à instância do Linux.

Se o sistema operacional do computador local for Linux ou macOS X

- [Cliente SSH \(p. 538\)](#)
- [EC2 Instance Connect \(p. 541\)](#)
- [AWS Systems Manager Session Manager do](#)

Se o sistema operacional do computador local for Windows

- [PuTTY \(p. 552\)](#)
- [Cliente SSH \(p. 538\)](#)
- [AWS Systems Manager Session Manager do](#)
- [Subsistema Windows para Linux \(p. 558\)](#)

### Pré-requisitos gerais para conectar-se à instância

Antes de se conectar à instância do Linux, verifique os seguintes pré-requisitos gerais:

- [Obter informações sobre a instância \(p. 535\)](#)
- [Habilitar o tráfego de entrada para a instância \(p. 537\)](#)
- [Encontrar a chave privada e definir as permissões \(p. 537\)](#)
- [\(Opcional\) Obter a impressão digital da instância \(p. 537\)](#)

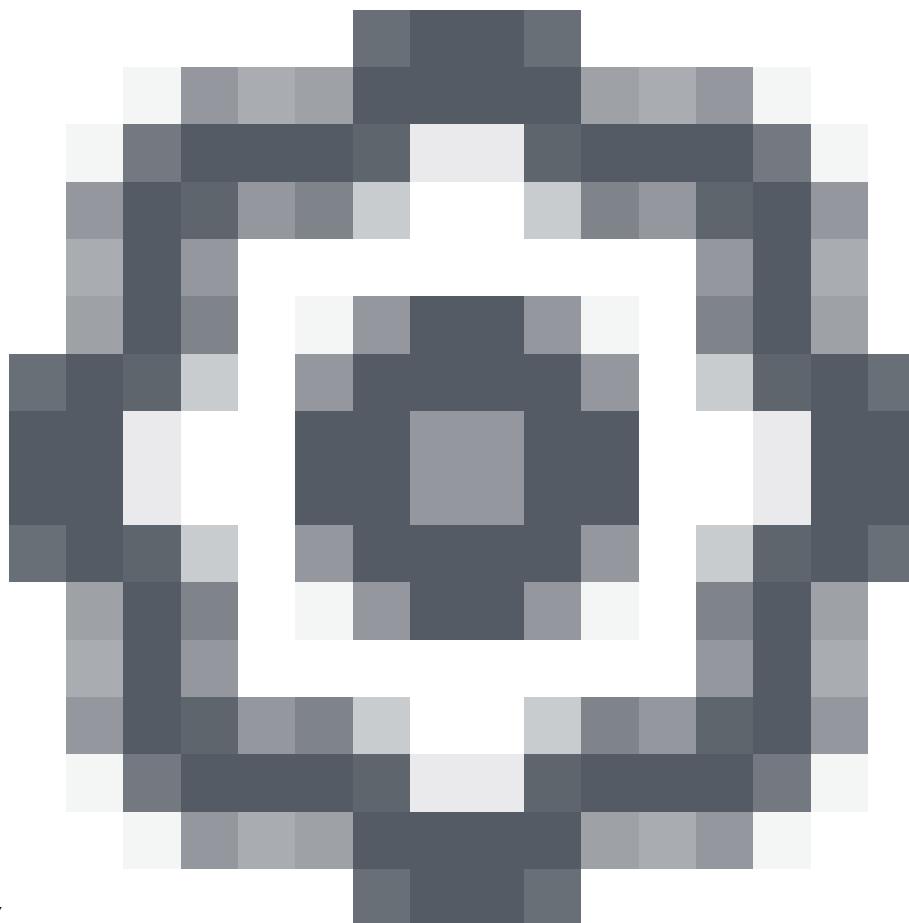
### Obter informações sobre a instância

- Obtenha o ID da instância.

Você pode obter o ID da instância usando o console do Amazon EC2 (na coluna ID da instância). Se preferir, você pode usar o comando [describe-instances](#) (AWS CLI) ou [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).

- Obtenha o nome do DNS público da instância.

Você pode obter o DNS público de sua instância usando o console do Amazon EC2. Consulte a coluna Public DNS (IPv4) (DNS público (IPv4)). Se esta coluna estiver oculta, escolha o ícone de configurações



( ) no canto superior direito da tela e selecionePublic DNS (IPv4) (DNS público (IPv4)). Se preferir, você pode usar o comando [describe-instances](#) (AWS CLI) ou [Get-EC2Instance](#) (AWS Tools for Windows PowerShell).

- (Somente IPv6) Obtenha o endereço IPv6 da instância.

Se você atribuiu um endereço IPv6 à sua instância, terá a opção de se conectar à sua instância usando seu endereço IPv6 em vez de um endereço IPv4 ou o nome de host DNS público. Seu computador local deve ter um endereço IPv6 e configurado para usar IPv6. Você pode obter o endereço IPv6 de sua instância usando o console do Amazon EC2. Verifique o campo IPv6 IPs (IPs IPv6). Se preferir, você pode usar o comando [describe-instances](#) (AWS CLI) ou [Get-EC2Instance](#) (AWS Tools for Windows PowerShell). Para obter mais informações sobre IPv6, consulte [Endereços IPv6 \(p. 939\)](#).

- Obtenha o nome de usuário para a instância.

É possível se conectar à instância usando o nome de usuário da conta de usuário ou o nome de usuário padrão da AMI usada para executar a instância.

- Obtenha o nome de usuário da sua conta de usuário.

Para obter mais informações sobre como criar uma conta de usuário, consulte [Gerenciar contas de usuário na instância do Amazon Linux \(p. 602\)](#).

- Obtenha o nome de usuário padrão da AMI usada para executar a instância:

- Para o Amazon Linux 2 ou a AMI do Amazon Linux, o nome do usuário é `ec2-user`.
- Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
- Para uma AMI do Ubuntu, o nome do usuário é `admin`.
- Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
- Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.

- Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
- Para uma AMI do Bitnami, o nome do usuário é `bitnami`.
- Caso contrário, verifique com o provedor da AMI.

## Habilitar o tráfego de entrada para a instância

- Permitir tráfego SSH de entrada do endereço IP à instância.

Verifique se o grupo de segurança associado à instância permite tráfego SSH de entrada do endereço IP. O grupo de segurança padrão para a VPC não permite o tráfego SSH de entrada por padrão. O grupo de segurança criado pelo assistente de execução de instância permite o tráfego SSH de entrada por padrão. Para obter mais informações, consulte [Autorizar tráfego de entrada para suas instâncias do Linux \(p. 1205\)](#).

## Encontrar a chave privada e definir as permissões

- 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 Linux em caso de perda da chave privada](#).

- Definir as permissões da chave privada

Se você usar um cliente SSH em um computador macOS ou Linux para conectar-se à instância do Linux, use o seguinte comando para definir as permissões do arquivo de chave privada de maneira que apenas você possa lê-lo.

```
chmod 400 my-key-pair.pem
```

Se você não definir essas permissões, não poderá conectar-se à instância usando esse par de chaves. Para obter mais informações, consulte [Erro: arquivo de chave privada desprotegido \(p. 1579\)](#).

## (Opcional) Obter a impressão digital da instância

Para se proteger de ataques "man-in-the-middle", você poderá verificar a impressão digital da chave RSA ao se conectar à instância. Verificar a impressão digital será útil se você tiver executado a instância a partir de uma AMI pública de terceiros.

Primeiro, obtenha a impressão digital da instância. Então, quando se conectar à instância, será solicitado que você verifique a impressão digital. É possível comparar a impressão digital obtida 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 à instância com confiança.

Pré-requisitos para obter a impressão digital da instância:

- Para obter a impressão digital da instância, você deve usar a AWS CLI. Para obter informações sobre como instalar a AWS CLI, consulte [Installing the AWS Command Line Interface \(Instalar a AWS Command Line Interface\)](#) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).

- A instância não deve estar no estado pending. A impressão digital só estará disponível após a conclusão da primeira inicialização da instância.

Para obter a impressão digital da instância

1. No computador local (e não na instância), use o comando [get-console-output](#) (AWS CLI) da seguinte maneira para obter a impressão digital:

```
aws ec2 get-console-output --instance-id instance_id --output text
```

2. Veja um exemplo do que você deve procurar na saída. A saída exata pode variar de acordo com o sistema operacional, a versão da AMI e se a AWS criou a chave.

```
ec2: #####  
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----  
ec2: 1024 SHA256:7HItIgTONZ/b0CH9c5Dq1ijgg06kFn86uQh05E/F9pU root@ip-10-0-2-182 (DSA)  
ec2: 256 SHA256:14UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY root@ip-10-0-2-182 (ECDSA)  
ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)  
ec2: 2048 SHA256:L816pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc root@ip-10-0-2-182 (RSA)  
ec2: -----END SSH HOST KEY FINGERPRINTS-----  
ec2: #####
```

## Conectar-se à instância do Linux usando SSH

Depois que iniciar sua instância, você poderá conectá-la e usá-la da forma como usaria um computador bem na sua frente.

As instruções a seguir explicam como se conectar à sua instância usando um cliente SSH. Se você receber um erro ao tentar se conectar à instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#). Para obter mais opções de conexão, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).

### Prerequisites

Antes de você se conectar à sua instância do Linux, preencha os pré-requisitos a seguir.

#### Verificar o status da instância

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se a instância passou nas verificações de status. É possível visualizar essas informações na coluna Status check (Verificação de status) na página Instances (Instâncias).

#### Obter o nome público do DNS e o nome de usuário para fazer a conexão à sua instância

Para localizar o nome público do DNS ou o endereço IP da instância e o nome de usuário que você deve usar para se conectar à instância, consulte [Pré-requisitos para se conectar à instância \(p. 535\)](#).

#### Encontrar a chave privada e definir as permissões

Para localizar a chave privada que é necessária para se conectar à sua instância e para definir as permissões de chave, consulte [Encontrar a chave privada e definir as permissões \(p. 537\)](#).

#### Instale um cliente SSH no computador local conforme necessário

O computador local pode ter um cliente SSH instalado por padrão. Isso pode ser verificado ao digitar ssh na linha de comando. Se o seu computador não reconhecer o comando, você pode instalar um cliente SSH.

- As versões recentes do Windows Server 2019 e do Windows 10 - OpenSSH estão incluídas como um componente instalável. Para obter mais informações, consulte [OpenSSH no Windows](#).

- Versões anteriores do Windows – baixe e instale o OpenSSH. Para obter mais informações, consulte [Win32-OpenSSH](#).
- Linux e macOS X – baixe e instale o OpenSSH. Para obter mais informações, consulte <https://www.openssh.com>.

## Conectar-se à instância do Linux usando um cliente SSH

Use o procedimento a seguir para se conectar à sua Instância do Linux usando um cliente SSH. Se você receber um erro ao tentar se conectar à instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#).

Para se conectar à sua instância usando SSH

1. Em uma janela do terminal, use o comando ssh para se conectar à instância. Especifique o caminho e o nome do arquivo da chave privada (.pem), o nome de usuário da instância e o nome DNS público ou o endereço IPv6 da instância. Para obter mais informações sobre como localizar a chave privada, o nome de usuário da instância e o nome DNS ou o endereço IPv6 de uma instância, consulte [Encontrar a chave privada e definir as permissões \(p. 537\)](#) e [Obter informações sobre a instância \(p. 535\)](#).

Para se conectar à instância, use um dos comandos a seguir.

- (DNS público) Para se conectar usando o nome DNS público da instância, insira o comando a seguir.

```
ssh -i /path/my-key-pair.pem my-instance-user-name@my-instance-public-dns-name
```

- (IPv6) Como alternativa, se sua instância tiver um endereço IPv6, para se conectar usando o endereço IPv6 da instância, digite o comando a seguir.

```
ssh -i /path/my-key-pair.pem my-instance-user-name@my-instance-IPv6-address
```

Você verá uma resposta como a seguinte:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'  
can't be established.  
ECDSA key fingerprint is 14UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.  
Are you sure you want to continue connecting (yes/no)?
```

2. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve anteriormente em [\(Opcional\) Obter a impressão digital da instância \(p. 537\)](#). Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
3. Digite **yes**.

Você verá uma resposta como a seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to the  
list of known hosts.
```

## Transfira arquivos para instâncias do Linux usando um cliente SCP

O protocolo de cópia segura (SCP) é uma das alternativas para transferir arquivos entre seu computador local e uma instância do Linux. Esta seção descreve como transferir arquivos com o SCP. O procedimento é semelhante ao procedimento de conexão a uma instância com o SSH.

## Prerequisites

- Verifique os pré-requisitos gerais para transferir arquivos à instância.

Os pré-requisitos gerais para transferir arquivos para uma instância são os mesmos que os pré-requisitos gerais para se conectar a uma instância. Para obter mais informações, consulte [Pré-requisitos gerais para conectar-se à instância \(p. 535\)](#).

- Instalação de um cliente SCP

A maioria dos computadores com Linux, Unix e Apple incluem um cliente SCP por padrão. Se seu não incluir, o projeto OpenSSH oferece implantação gráts do pacote completo das ferramentas SSH, inclusive um cliente SCP. Para obter mais informações, consulte <https://www.openssh.com>.

O procedimento a seguir acompanha o uso do SCP para transferir um arquivo usando o nome DNS público da instância ou o endereço IPv6 se sua instância tiver um.

Para usar o SCP para transferir arquivos entre o computador e a sua instância

1. Determine a localização do arquivo de origem no seu computador e o caminho de destino na instância. Nos exemplos a seguir, o nome do arquivo de chave privada é `my-key-pair.pem`, o arquivo a ser transferido é `my-file.txt`, o nome de usuário da instância é `ec2-user`, o nome de DNS público da instância é `my-instance-public-dns-name` e o endereço IPv6 da instância é `my-instance-IPv6-address`.
  - (DNS público) Para transferir um arquivo para o destino na instância, insira o seguinte comando do seu computador.

```
scp -i /path/my-key-pair.pem /path/my-file.txt ec2-user@my-instance-public-dns-name:path/
```

- (IPv6) Para transferir um arquivo para o destino na instância, se ela tiver um endereço IPv6, insira o seguinte comando no seu computador. O endereço IPv6 deve vir entre colchetes ([ ]), que devem ser recuados (\).

```
scp -i /path/my-key-pair.pem /path/my-file.txt ec2-user@[my-instance-IPv6-address]:path/
```

2. Se ainda não tiver conectado à instância usando SSH, você verá uma resposta como a seguinte:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)' can't be established.  
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.  
Are you sure you want to continue connecting (yes/no)?
```

(Opcional) Você também pode verificar se a impressão digital no alerta de segurança corresponde à impressão digital da instância. Para obter mais informações, consulte [\(Opcional\) Obter a impressão digital da instância \(p. 537\)](#).

Digite `yes`.

3. Se a transferência for bem-sucedida, a resposta será semelhante à seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)  
to the list of known hosts.  
my-file.txt 100% 480 24.4KB/s 00:00
```

4. Para transferir um arquivo na outra direção (de uma instância do Amazon EC2 para o seu computador), basta inverter a ordem dos parâmetros do host. Por exemplo, você pode transferir o `my-`

`file.txt` da instância do EC2 para um destino no seu computador local `my-file2.txt`, conforme exibido nos exemplos a seguir.

- (DNS Público) Para transferir um arquivo para um destino no seu computador, insira o seguinte comando do seu computador.

```
scp -i /path/my-key-pair.pem ec2-user@my-instance-public-dns-name:path/my-file.txt  
path/my-file2.txt
```

- (IPv6) Para transferir um arquivo para um destino no computador se a instância tiver um endereço IPv6, insira o seguinte comando do seu computador. O endereço IPv6 deve vir entre colchetes ([ ]), que devem ser recuados (\).

```
scp -i /path/my-key-pair.pem ec2-user@[my-instance-IPv6-address\]:path/my-file.txt  
path/my-file2.txt
```

## Conectar-se à instância do Linux usando EC2 Instance Connect

O Amazon EC2 Instance Connect fornece uma forma simples e segura de conexão às instâncias do Linux usando Secure Shell (SSH). Com o EC2 Instance Connect, você usa políticas do AWS Identity and Access Management (IAM) e principais para controlar o acesso de SSH às suas instâncias, eliminando a necessidade de compartilhar e gerenciar as chaves de SSH. Todas as solicitações de conexão usando o EC2 Instance Connect são registradas no AWS CloudTrail para que você possa auditar as solicitações de conexão ([p. 921](#)).

Você pode usar o EC2 Instance Connect para se conectar às instâncias do Linux usando o console do Amazon EC2 (cliente baseado em navegador), a CLI do Amazon EC2 Instance Connect ou o cliente SSH de sua escolha.

Ao conectar-se a uma instância usando o EC2 Instance Connect, a API do Instance Connect envia por push e uma chave pública SSH de uso único para os [metadados da instância \(p. 649\)](#), onde ela permanece por 60 segundos. A política do IAM anexada ao usuário do IAM autoriza seu usuário do IAM a enviar por push a chave pública para os metadados da instância. O daemon SSH usa `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser`, que são configurados quando o Instance Connect é instalado, para procurar a chave pública dos metadados da instância para autenticação e conectar você à instância.

Você pode usar EC2 Instance Connect para se conectar a instâncias que têm endereços IP públicos ou privados. Para obter mais informações, consulte [Conectar-se usando EC2 Instance Connect \(p. 548\)](#).

### Tip

Se estiver se conectando a uma instância do Linux em um computador local que executa o Windows, consulte a documentação a seguir:

- [Conectar-se à instância do Linux no Windows usando PuTTY \(p. 552\)](#)
- [Conectar-se à instância do Linux usando SSH \(p. 538\)](#)
- [Conectar-se à instância do Linux no Windows usando o Subsistema Windows para Linux \(p. 558\)](#)

### Tópicos

- [Configurar o EC2 Instance Connect \(p. 542\)](#)
- [Conectar-se usando EC2 Instance Connect \(p. 548\)](#)
- [Desinstalar o EC2 Instance Connect \(p. 551\)](#)

## Configurar o EC2 Instance Connect

Para usar o EC2 Instance Connect para se conectar a uma instância, você precisa configurar todas as instâncias compatíveis usando o Instance Connect (este é um requisito único para cada instância) e será necessário conceder permissão para todos os principais do IAM que usarem o Instance Connect. Depois de concluir as tarefas de configuração a seguir, você pode [se conectar à sua instância usando EC2 Instance Connect \(p. 548\)](#).

### Tarefas para configurar o EC2 Instance Connect

- [Tarefa 1: configurar o acesso à rede para uma instância \(p. 542\)](#)
- [Tarefa 2: \(condicional\) instalar o EC2 Instance Connect em uma instância \(p. 543\)](#)
- [Tarefa 3: \(opcional\) instalar a CLI do EC2 Instance Connect no seu computador \(p. 545\)](#)
- [Tarefa 4: configurar permissões do IAM para o EC2 Instance Connect \(p. 546\)](#)

Para obter mais informações sobre como configurar o EC2 Instance Connect, consulte [Proteger os bastion hosts com o Amazon EC2 Instance Connect](#).

### Limitations

- Você pode instalar o EC2 Instance Connect nas seguintes distribuições compatíveis do Linux:
  - Amazon Linux 2 (qualquer versão)
  - Ubuntu 16.04 ou posterior
- Se você definiu as configurações de `AuthorizedKeysCommand` e `AuthorizedKeysCommandUser` para a autenticação SSH, a instalação do EC2 Instance Connect não as atualizará. Consequentemente, não será possível usar o Instance Connect.

### Pré-requisitos para a instalação EC2 Instance Connect

- Verifique os pré-requisitos gerais para se conectar à instância usando SSH.  
Para obter mais informações, consulte [Pré-requisitos gerais para conectar-se à instância \(p. 535\)](#).
- Instale um cliente SSH no computador local.

É muito provável que seu computador local tenha um cliente SSH instalado por padrão. Você pode verificar se existe um cliente SSH digitando `ssh` na linha de comando. Se o seu computador local não reconhecer o comando, você poderá instalar um cliente SSH. Para obter informações sobre como instalar um cliente SSH no Linux ou macOS X, consulte <http://www.openssh.com>. Para obter informações sobre como instalar um cliente SSH no Windows 10, consulte [OpenSSH no Windows](#).

- Instale a AWS CLI no computador local.

Para configurar as permissões do IAM, é necessário usar a AWS CLI. Para obter informações sobre como instalar ou atualizar a AWS CLI, consulte [Installing the AWS CLI \(Instalar a AWS CLI\)](#) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).

- [Ubuntu] Instale a AWS CLI em sua instância.

Para instalar o EC2 Instance Connect em uma instância do Ubuntu, use a AWS CLI na instância. Para obter informações sobre como instalar ou atualizar a AWS CLI, consulte [Installing the AWS CLI \(Instalar a AWS CLI\)](#) no AWS Command Line Interface User Guide (Manual do usuário da AWS Command Line Interface).

### Tarefa 1: configurar o acesso à rede para uma instância

Você deve configurar o seguinte acesso à rede para que seus usuários possam se conectar à instância usando EC2 Instance Connect:

- Caso seus usuários acessem sua instância pela Internet, ela deverá ter um endereço IP público e estar em uma sub-rede pública. Para obter mais informações, consulte [Habilitar o acesso à Internet](#) no Manual do usuário da Amazon VPC.
- Caso seus usuários acessem sua instância por meio do endereço IP privado da instância, você deverá estabelecer uma conectividade de rede privada com sua VPC, por meio do AWS Direct Connect, do VPN de local a local da AWS ou do emparelhamento da VPC, para que seus usuários possam acessar o endereço IP privado da instância.
- Certifique-se de que o grupo de segurança associado à sua instância [permite tráfego SSH de entrada \(p. 1206\)](#) na porta 22 a partir do seu endereço IP ou da rede. O grupo de segurança padrão para a VPC não permite o tráfego SSH de entrada por padrão. O grupo de segurança criado pelo assistente de execução permite o tráfego SSH de entrada por padrão. Para obter mais informações, consulte [Autorizar tráfego de entrada para suas instâncias do Linux \(p. 1205\)](#).
- (Cliente baseado no navegador do console do Amazon EC2) Certifique-se de que o grupo de segurança associado à instância permita tráfego SSH de entrada da faixa de endereços IP para esse serviço. Para identificar o intervalo de endereços, faça download do arquivo JSON fornecido pela AWS e filtre para o subconjunto do EC2 Instance Connect, usando `EC2_INSTANCE_CONNECT` como valor do serviço. Para obter mais informações sobre como fazer download do arquivo JSON e filtrar por serviço, consulte [Intervalos de endereços IP da AWS](#) em Referência geral da Amazon Web Services.

## Tarefa 2: (condicional) instalar o EC2 Instance Connect em uma instância

Você pode ignorar essa tarefa, caso tenha usado uma das seguintes AMIs para iniciar sua instância, pois elas vêm pré-instaladas com o EC2 Instance Connect:

- Amazon Linux 2 2.0.20190618 ou posterior
- Ubuntu 20.04 ou posterior

Para versões anteriores dessas AMIs, você deverá instalar o Instance Connect em todas as instâncias que vão oferecer suporte à conexão usando o Instance Connect.

Instalar o Instance Connect configura o daemon SSH na instância. O procedimento de instalação do Instance Connect é diferente para instâncias em execução que usem o Amazon Linux 2 e o Ubuntu.

### Amazon Linux 2

#### Para instalar EC2 Instance Connect em uma instância aberta com Amazon Linux 2

1. Conecte-se à sua instância usando SSH.

Use o par de chaves de SSH atribuído à sua instância ao abri-la e o nome do usuário padrão da AMI usada para abrir a instância. Para Amazon Linux 2, o nome do usuário padrão é `ec2-user`.

Por exemplo, se a instância tiver sido executada usando o Amazon Linux 2, o nome DNS público da instância for `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e o par de chaves for `my_ec2_private_key.pem`, use o seguinte comando para o SSH na instância:

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Para obter mais informações sobre como se conectar à sua instância, consulte [Conectar-se à instância do Linux usando SSH \(p. 538\)](#).

2. Instale o pacote EC2 Instance Connect na sua instância.

Para Amazon Linux 2, use o comando `yum install`.

```
[ec2-user ~]$ sudo yum install ec2-instance-connect
```

Deverão ser visíveis quatro novos arquivos na pasta /opt/aws/bin/:

```
eic_curlAuthorizedKeys  
eic_harvestHostkeys  
eic_parseAuthorizedKeys  
eic_runAuthorizedKeys
```

3. (Opcional) Verifique se o Instance Connect foi instalando com sucesso na sua instância.

Use o comando sudo less para verificar se o arquivo /etc/ssh/sshd\_config foi atualizado corretamente, da seguinte forma:

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config
```

O Instance Connect foi instalado com sucesso se as linhas AuthorizedKeysCommand e AuthorizedKeysCommandUser do /etc/ssh/sshd\_config contiverem os seguintes valores:

```
AuthorizedKeysCommand /opt/aws/bin/eic_runAuthorizedKeys %u %f  
AuthorizedKeysCommandUser ec2-instance-connect
```

- O AuthorizedKeysCommand define o script eic\_runAuthorizedKeys para buscar as chaves nos metadados da instância
- AuthorizedKeysCommandUser O define o usuário do sistema como ec2-instance-connect

#### Note

Se você tiver previamente configurado AuthorizedKeysCommand e AuthorizedKeysCommandUser, a instalação do Instance Connect não mudará os valores e você não poderá usar Instance Connect.

#### Ubuntu

Para instalar o EC2 Instance Connect em uma instância aberta com Ubuntu 16.04 ou posterior

1. Conecte-se à sua instância usando SSH.

Use o par de chaves de SSH atribuído à sua instância ao abri-la e use o nome do usuário padrão da AMI usada para abrir a instância. Para uma AMI do Ubuntu, o nome de usuário é ubuntu.

Por exemplo, se a instância tiver sido executada usando Ubuntu, o nome DNS público da instância for ec2-a-b-c-d.us-west-2.compute.amazonaws.com e o par de chaves for my\_ec2\_private\_key.pem, use o seguinte comando para o SSH na instância:

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Para obter mais informações sobre como se conectar à sua instância, consulte [Conectar-se à instância do Linux usando SSH \(p. 538\)](#).

2. (Opcional) Garanta que sua instância tenha a AMI do Ubuntu mais recente.

Para Ubuntu, use os seguintes comandos para atualizar todos os pacotes na instância.

```
ubuntu:~$ sudo apt-get update
```

```
ubuntu:~$ sudo apt-get upgrade
```

3. Instale o pacote Instance Connect na sua instância.

Para o Ubuntu, use o comando sudo apt-get.

```
ubuntu:~$ sudo apt-get install ec2-instance-connect
```

Deverão ser visíveis quatro novos arquivos na pasta /usr/share/ec2-instance-connect/:

```
eic_curlAuthorizedKeys  
eic_harvestHostkeys  
eic_parseAuthorizedKeys  
eic_runAuthorizedKeys
```

4. (Opcional) Verifique se o Instance Connect foi instalado com sucesso na sua instância.

Use o comando sudo less para verificar se o /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf foi atualizado corretamente, da seguinte forma:

```
ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

O Instance Connect foi instalado com sucesso se as linhas AuthorizedKeysCommand e AuthorizedKeysCommandUser do /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf contiverem os seguintes valores:

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_runAuthorizedKeys %u %f  
AuthorizedKeysCommandUser ec2-instance-connect
```

- O AuthorizedKeysCommand define o script eic\_runAuthorizedKeys para buscar as chaves nos metadados da instância
- AuthorizedKeysCommandUser O define o usuário do sistema como ec2-instance-connect

#### Note

Se você tiver previamente configurado AuthorizedKeysCommand e AuthorizedKeysCommandUser, a instalação do Instance Connect não mudará os valores e você não poderá usar Instance Connect.

Para obter mais informações sobre o pacote do EC2 Instance Connect, consulte [aws/aws-ec2-instance-connect-config](#) no site do GitHub.

#### Tarefa 3: (opcional) instalar a CLI do EC2 Instance Connect no seu computador

A CLI do EC2 Instance Connect fornece uma experiência simplificada para se conectar a instâncias do EC2 por meio de um único comando, `mssh instance_id`. Para obter mais informações, consulte [Conectar-se usando a CLI do EC2 Instance Connect \(p. 549\)](#).

## Note

Não há necessidade de instalar a CLI do EC2 Instance Connect se os usuários só usarem o console da Amazon EC2 (cliente com base em navegador) ou um cliente SSH para se conectar a uma instância.

### Como instalar o pacote da CLI do EC2 Instance Connect

Use [pip](#) para instalar o pacote `ec2instanceconnectcli`. Para obter mais informações, consulte [aws/aws-ec2-instance-connect-cli](#) no site do GitHub e <https://pypi.org/project/ec2instanceconnectcli/> no site de índices de pacotes do Python (PyPI).

```
$ pip install ec2instanceconnectcli
```

### Tarefa 4: configurar permissões do IAM para o EC2 Instance Connect

Para que os principais do IAM se conectem a uma instância usando o EC2 Instance Connect, é necessário conceder a eles a permissão necessária para enviar a chave pública para a instância. Conceda a eles a permissão criando uma política do IAM e anexando a política aos principais do IAM que exigem a permissão. Para obter mais informações, consulte [Ações, recursos e chaves de condição para o Amazon EC2 Instance Connect](#).

As instruções a seguir explicam como criar a política e anexá-la a um usuário do IAM usando a AWS CLI. A mesma política pode ser aplicada a outros principais do IAM como funções do IAM. Para obter instruções que usam o AWS Management Console, consulte [Creating IAM policies \(console\)](#) ([Criar políticas do IAM \(console\)](#)), [Adding permissions by attaching policies directly to the user](#) ([Adicionar permissões anexando políticas diretamente ao usuário](#)) e [Creating IAM roles](#) ([Criar funções do IAM](#)) no IAM User Guide (Manual do usuário do IAM).

Para conceder uma permissão do principal do IAM para EC2 Instance Connect (AWS CLI)

1. Crie um documento de política JSON que inclua o seguinte conteúdo para a nova política:

- A ação `ec2-instance-connect:SendSSHPublicKey`. Isso concede ao principal do IAM permissão para enviar a chave pública a uma instância. Com `ec2-instance-connect:SendSSHPublicKey`, considere restringir o acesso a instâncias do EC2 específicas. Caso contrário, todos os principais do IAM com essa permissão poderão se conectar a todas as instâncias do EC2. Você também pode restringir o acesso especificando ARNs de recursos ou usando tags de recurso como [chaves de condição](#).
- A condição `ec2:osuser`. Isso especifica o nome do usuário do sistema operacional que pode enviar por push a chave pública a uma instância. Use o nome de usuário padrão para a AMI que você usou para executar a instância. O nome de usuário padrão para o Amazon Linux 2 é `ec2-user` e `ubuntu`, para o Ubuntu.
- A ação `ec2:DescribeInstances`. Isso é necessário ao usar a CLI do EC2 Instance Connect porque o wrapper chama essa ação. Os principais do IAM talvez já tenham permissão para chamar essa ação a partir de outra política.

Veja abaixo um exemplo de documento de política. É possível omitir a instrução para a ação `ec2:DescribeInstances` se os seus usuários usarem somente um cliente SSH para se conectar às instâncias. Você pode substituir as instâncias especificadas em `Resource` pelo curinga `*` para conceder aos usuários o acesso a todas as instâncias do EC2 usando o EC2 Instance Connect.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {
```

```
"Effect": "Allow",
"Action": "ec2-instance-connect:SendSSHPublicKey",
"Resource": [
    "arn:aws:ec2:region:account-id:instance/i-1234567890abcdef0",
    "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
],
"Condition": {
    "StringEquals": {
        "ec2:osuser": "ami-username"
    }
},
{
    "Effect": "Allow",
    "Action": "ec2:DescribeInstances",
    "Resource": "*"
}
]
```

A política anterior permite o acesso a instâncias específicas, identificadas por seu ID de instância. Como alternativa, é possível usar tags de recurso para controlar o acesso a 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 acesse uma instância somente se essa instância tiver uma tag de recurso com chave=tag-key e valor=tag-value. 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 IAM User Guide (Manual do usuário do IAM).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/tag-key": "tag-value"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

2. Use o comando [create-policy](#) para criar uma nova política gerenciada e especifique o documento JSON que você criou para usar como conteúdo para a nova política.

```
$ aws iam create-policy --policy-name my-policy --policy-document file://JSON-file-name
```

3. Use o comando [attach-user-policy](#) para associar a política gerenciada especificada ao usuário do IAM especificado. No parâmetro **--user-name**, especifique o nome amigável (não o ARN) do usuário do IAM.

```
$ aws iam attach-user-policy --policy-arn arn:aws:iam::account-id:policy/my-policy --user-name IAM-friendly-name
```

## Conectar-se usando EC2 Instance Connect

As instruções a seguir explicam como se conectar à sua instância do Linux usando o EC2 Instance Connect.

Se você receber uma mensagem de erro ao tentar se conectar à sua instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#) e [Como solucionar problemas de conexão à minha instância do EC2 usando o EC2 Instance Connect?](#).

### Tópicos

- [Limitations \(p. 548\)](#)
- [Prerequisites \(p. 548\)](#)
- [Conectar-se usando EC2 Instance Connect \(p. 548\)](#)

### Limitations

- As seguintes distribuições do Linux são compatíveis:
  - Amazon Linux 2 (qualquer versão)
  - Ubuntu 16.04 ou posterior
- Para se conectar usando o console da Amazon EC2 (cliente baseado em navegador), a instância deve ter um endereço IPv4 público.
- Se a instância não tiver um endereço IP público, você poderá se conectar à instância usando um cliente SSH ou a CLI do EC2 Instance Connect. Por exemplo, é possível se conectar de dentro da mesma VPC ou por meio de uma conexão VPN, de um gateway de trânsito ou do AWS Direct Connect.
- O EC2 Instance Connect não oferece suporte à conexão usando um endereço IPv6.

### Prerequisites

- Instale o Instance Connect na sua instância.  
Para obter mais informações, consulte [Configurar o EC2 Instance Connect \(p. 542\)](#).
- (Opcional) Instale um cliente SSH no computador local.

Não há necessidade de instalar o cliente SSH se os usuários só usarem o console da EC2 Instance Connect (cliente baseado em navegador) ou a CLI do Amazon EC2 para se conectarem a uma instância. É muito provável que seu computador local tenha um cliente SSH instalado por padrão. Você pode verificar se existe um cliente SSH digitando ssh na linha de comando. Se o seu computador local não reconhecer o comando, você poderá instalar um cliente SSH. Para obter informações sobre como instalar um cliente SSH no Linux ou macOS X, consulte <http://www.openssh.com>. Para obter informações sobre como instalar um cliente SSH no Windows 10, consulte [OpenSSH no Windows](#).

- (Opcional) Instale a CLI do EC2 Instance Connect CLI no computador local.

Não há necessidade de instalar a CLI do EC2 Instance Connect se os usuários só usarem o console da Amazon EC2 (cliente baseado em navegador) ou um cliente SSH para se conectar a uma instância. Para obter mais informações, consulte [Tarefa 3: \(opcional\) instalar a CLI do EC2 Instance Connect no seu computador \(p. 545\)](#). Esse método de conexão funciona para instâncias com endereços IP públicos.

### Conectar-se usando EC2 Instance Connect

#### Opções

- [Conectar-se usando o console da Amazon EC2 \(cliente baseado em navegador\) \(p. 549\)](#)
- [Conectar-se usando a CLI do EC2 Instance Connect \(p. 549\)](#)

- [Conectar-se usando sua própria chave e cliente SSH \(p. 550\)](#)

### [Conectar-se usando o console da Amazon EC2 \(cliente baseado em navegador\)](#)

Você pode se conectar a uma instância usando o console da Amazon EC2 (cliente baseado em navegador) selecionando a instância no console e optando por se conectar usando o EC2 Instance Connect. O Instance Connect lida com as permissões e fornece uma conexão bem-sucedida.

Como conectar-se à sua instância usando o cliente com base em navegador 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. Selecione EC2 Instance Connect.
5. Verifique o nome de usuário e escolha Connect (Conectar) para abrir uma janela de terminal.

### [Conectar-se usando a CLI do EC2 Instance Connect](#)

Você pode se conectar a uma instância usando a CLI do EC2 Instance Connect CLI fornecendo somente o ID da instância, enquanto a CLI do Instance Connect executa as três ações a seguir em uma só chamada: gera uma chave pública do SSH de uso único, envia por push a chave para a instância, onde permanece por 60 segundos, e conecta o usuário à instância. Você pode usar comandos básicos de SSH/SFTP com a CLI do Instance Connect.

Esse método de conexão funciona para instâncias com endereços IP públicos e privados. Ao se conectar a uma instância que tenha apenas endereços IP privados, o computador local a partir do qual você está iniciando a sessão deve ter conectividade com o endpoint do serviço EC2 Instance Connect (para enviar sua chave pública SSH à instância), bem como conectividade de rede com o endereço IP privado da instância. O endpoint de serviço do EC2 Instance Connect é acessível pela Internet ou por meio de uma interface virtual pública do AWS Direct Connect. Para se conectar ao endereço IP privado da instância, você pode aproveitar serviços, como [AWS Direct Connect](#), [AWS Site-to-Site VPN](#) ou [emparelhamento de VPC](#).

#### Note

`-i` não é compatível ao usar mssh. Ao usar o comando mssh para se conectar à instância, você não precisa especificar nenhum tipo de arquivo de identidade porque Instance Connect gerencia o par de chaves.

#### Amazon Linux 2

##### [Como se conectar a uma instância usando a CLI do EC2 Instance Connect](#)

Use o comando mssh com o ID da instância conforme a seguir. Não é necessário especificar o nome de usuário para a AMI.

```
$ mssh i-001234a4bf70dec41EXAMPLE
```

#### Ubuntu

##### [Como se conectar a uma instância usando a CLI do EC2 Instance Connect](#)

Use o comando mssh com o ID da instância e o nome de usuário padrão para a AMI do Ubuntu conforme a seguir. É necessário especificar o nome de usuário para a AMI ou você obterá o seguinte erro: Falha na autenticação.

```
$ mssh ubuntu@i-001234a4bf70dec41EXAMPLE
```

## Conectar-se usando sua própria chave e cliente SSH

Você pode usar sua própria chave SSH e conectar-se à sua instância a partir do cliente SSH de sua escolha enquanto usa a API do EC2 Instance Connect. Isso permite que você se beneficie da capacidade do Instance Connect de enviar por push uma chave pública para a instância. Esse método de conexão funciona para instâncias com endereços IP públicos e privados.

### Requirements

- Os tipos de chave RSA com suporte são OpenSSH e SSH2. Os tamanhos compatíveis são 2.048 e 4.096. Para obter mais informações, consulte [Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2](#) (p. 1212).
- Ao se conectar a uma instância que só tenha endereços IP privados, o computador local a partir do qual você está iniciando a sessão SSH deve ter conectividade com o endpoint do serviço EC2 Instance Connect (para enviar sua chave pública SSH para a instância), além de conectividade de rede para o endereço IP privado da instância para estabelecer a sessão SSH. O endpoint de serviço do EC2 Instance Connect é acessível pela Internet ou por meio de uma interface virtual pública do AWS Direct Connect. Para se conectar ao endereço IP privado da instância, você pode aproveitar serviços, como [AWS Direct Connect](#), [AWS Site-to-Site VPN](#) ou [emparelhamento de VPC](#).

Para se conectar à sua instância usando a própria chave e qualquer cliente SSH

1. (Opcional) Gerar chaves novas chaves SSH privadas e públicas

Você pode gerar novas chaves SSH públicas e privadas, `my_rsa_key` e `my_rsa_key.pub`, usando o comando a seguir:

```
$ ssh-keygen -t rsa -f my_rsa_key
```

2. Envie por push a chave pública do SSH para a instância

Use o comando `send-ssh-public-key` para enviar a chave pública SSH para a instância. Se você tiver lançado sua instância usando Amazon Linux 2, o nome do usuário padrão para a AMI será `ec2-user`. Se você tiver lançado sua instância usando Ubuntu, o nome do usuário padrão para a AMI será `ubuntu`.

O exemplo a seguir envia a chave pública para a instância especificada na zona de disponibilidade especificada, para autenticar `ec2-user`:

```
$ aws ec2-instance-connect send-ssh-public-key \
  --instance-id i-001234a4bf70dec41EXAMPLE \
  --availability-zone us-west-2b \
  --instance-os-user ec2-user \
  --ssh-public-key file://my_rsa_key.pub
```

3. Conecte-se à instância usando a chave privada

Use o comando `ssh` para se conectar à instância usando a chave privada antes de a chave pública ser removida dos metadados da instância (você tem 60 segundos antes de ser removida). Especifique a chave privada que corresponde à chave pública, ao nome de usuário padrão da AMI que você usou para executar sua instância e o nome DNS público da instância (se estiver se conectando por uma rede privada, especifique o nome DNS privado ou o endereço IP). Adicione a opção `IdentitiesOnly=yes` para garantir que apenas os arquivos na configuração `ssh` e a chave especificada sejam usados para a conexão.

```
$ ssh -o "IdentitiesOnly=yes" -i my_rsa_key ec2-  
user@ec2-198-51-100-1.compute-1.amazonaws.com
```

## Desinstalar o EC2 Instance Connect

Para desabilitar o EC2 Instance Connect, conecte-se à sua instância e desinstale o pacote `ec2-instance-connect` que você instalou no SO. Se a configuração `sshd` corresponder ao que foi definido quando você instalou o EC2 Instance Connect, desinstalar o pacote `ec2-instance-connect` também removerá a configuração `sshd`. Se a configuração `sshd` tiver sido modificada após a instalação do EC2 Instance Connect, você deverá atualizá-la manualmente.

### Amazon Linux 2

Você pode desinstalar o EC2 Instance Connect no Amazon Linux 2 2.0.20190618 ou posterior, em que o EC2 Instance Connect está pré-configurado.

Para desinstalar o EC2 Instance Connect em uma instância executada com o Amazon Linux 2

1. Conecte-se à sua instância usando SSH. Especifique o par de chaves SSH usado para sua instância quando você a executou e o nome de usuário padrão para a AMI do Amazon Linux 2, que é `ec2-user`.

Por exemplo. o comando `ssh` conecta-se à instância com o nome DNS público `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, usando o par de chaves `my_ec2_private_key.pem`.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-  
west-2.compute.amazonaws.com
```

2. Desinstale o pacote `ec2-instance-connect` usando o comando `yum`.

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

### Ubuntu

Como desinstalar o EC2 Instance Connect em uma instância executada com uma AMI do Ubuntu

1. Conecte-se à sua instância usando SSH. Especifique o par de chaves SSH usado para sua instância quando você a executou e o nome de usuário padrão para a AMI do Ubuntu, que é `ubuntu`.

Por exemplo. o comando `ssh` conecta-se à instância com o nome DNS público `ec2-a-b-c-d.us-west-2.compute.amazonaws.com`, usando o par de chaves `my_ec2_private_key.pem`.

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

2. Desinstale o pacote `ec2-instance-connect` usando o comando `apt-get`.

```
ubuntu:~$ sudo apt-get remove ec2-instance-connect
```

## Conectar-se à instância do Linux no Windows usando PuTTY

Depois que iniciar sua instância, você poderá conectá-la e usá-la da forma como usaria um computador bem na sua frente.

As instruções a seguir explicam como se conectar à sua instância usando PuTTY, um cliente SSH gratuito para Windows. Se você receber um erro ao tentar se conectar à instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#).

### Prerequisites

Antes de você se conectar à sua instância do Linux usando o PuTTY, preencha os pré-requisitos a seguir.

Verifique se a instância está pronta

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se a instância passou nas verificações de status. É possível visualizar essas informações na coluna Status check (Verificação de status) na página Instances (Instâncias).

Verifique os pré-requisitos gerais para se conectar à instância

Para localizar o nome DNS público ou o endereço IP da instância e o nome de usuário que você deve usar para se conectar à instância, consulte [Pré-requisitos gerais para conectar-se à instância \(p. 535\)](#).

Instale o PuTTY no computador local

Faça download e instale o PuTTY pela [página de download do PuTTY](#). Se você já tiver uma versão mais antiga do PuTTY instalada, recomendamos fazer download da versão mais recente. Instale o pacote inteiro.

Converta a chave privada usando o PuTTYgen

Localize a chave privada (arquivo .pem) para o par de chaves que especificou quando iniciou a instância. Converta o arquivo .pem para um arquivo .ppk para uso com o PuTTY. Para obter mais informações, siga as etapas da próxima seção.

### Converta a chave privada usando o PuTTYgen

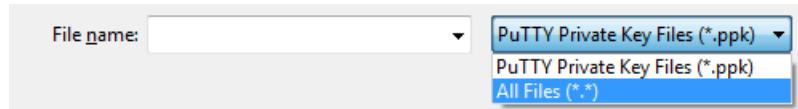
O PuTTY não é originalmente compatível com o formato de chave privada para chaves SSH. O PuTTY fornece uma ferramenta chamada PuTTYgen, que converte as chaves para o formato necessário para PuTTY. Você deve converter sua chave privada (arquivo .pem) nesse formato (arquivo .ppk) conforme a seguir para conectar à sua instância usando PuTTY.

Para converter sua chave privada

1. No menu Start (Iniciar), selecione All Programs (Todos os programas), PuTTY, PuTTYgen.
2. Em Tipo de chave a ser gerada, escolha RSA. Se a sua versão de PuTTYgen não inclui esta opção, escolha SSH-2 RSA.



3. Escolha Load (Carregar). Por padrão, o PuTTYgen exibe somente arquivos com a extensão .ppk. Para localizar o arquivo .pem, escolha a opção para exibir arquivos de todos os tipos.



4. Selecione o arquivo `.pem` para o par de chaves que você especificou ao executar a instância e selecione Open (Abrir). A PuTTYgen exibe um aviso de que o arquivo `.pem` foi importado com êxito. Escolha OK.
5. Escolha Save private key (Salvar chave privada) para salvar a chave no formato PuTTY. A PuTTYgen exibe um aviso sobre salvar a chave sem uma senha. Escolha Sim.

Note

Uma senha em uma chave privada é uma camada extra de proteção. Mesmo se a chave privada for descoberta, ela não pode ser usada sem a senha. A desvantagem de se usar uma senha é que a automação se torna mais difícil porque a intervenção humana é necessária para fazer logon a uma instância, ou para copiar arquivos a uma instância.

6. Especifique o mesmo nome da chave usado para o par de chaves (por exemplo, `my-key-pair`) e escolha Save (Salvar). O PuTTY adiciona automaticamente a extensão de arquivo `.ppk`.

Sua chave privada está agora no formato correto para uso com o PuTTY. Agora você pode conectar a sua instância usando o cliente SSH do PuTTY.

## Conecte-se à sua instância do Linux

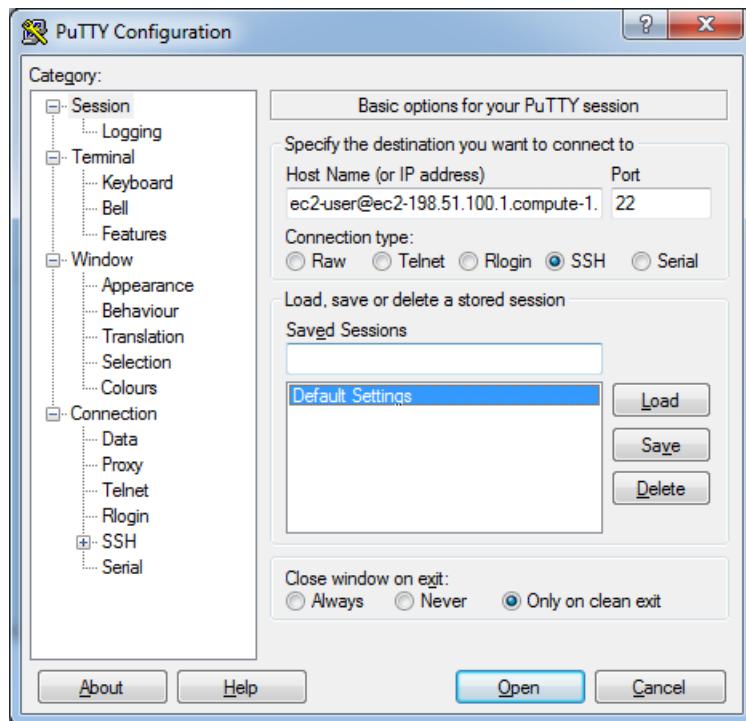
Use o procedimento a seguir para se conectar à sua Instância do Linux usando o PuTTY. Você precisa do arquivo `.ppk` que criou para sua chave privada. Para obter mais informações, consulte [Converte a chave privada usando o PuTTYgen \(p. 552\)](#) na seção anterior. Se você receber um erro ao tentar se conectar à instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#).

### Para se conectar à instância usando PuTTY

1. Inicie o PuTTY (no menu Start (Iniciar), selecione All Programs (Todos os programas), PuTTY, PuTTY).
2. No painel Categoria, selecione Sessão e preencha os seguintes campos:
  - a. Na caixa Host Name (Nome do host), execute uma das ações a seguir:
    - (DNS Público) Para se conectar usando o nome DNS público da instância, insira `my-instance-user-name@my-instance-public-dns-name`.
    - (IPv6) Como alternativa, se a instância tiver um endereço IPv6, para se conectar usando o endereço IPv6 da instância, insira `my-instance-user-name@my-instance-IPv6-address`.

Para obter informações sobre como obter o nome de usuário da instância e o nome DNS público ou o endereço IPv6 da instância, consulte [Obter informações sobre a instância \(p. 535\)](#).

- b. Verifique se o valor do Port é 22.
- c. Em Tipo de conexão, selecione SSH.



3. (Opcional) Você pode configurar o PuTTY para enviar automaticamente dados "keepalive" em intervalos regulares para manter a sessão ativa. Isso é útil para evitar a desconexão da instância por inatividade da sessão. No painel Category, escolha Connection e insira o intervalo necessário no campo Seconds between keepalives. Por exemplo, se a sessão desconectar após 10 minutos de inatividade, insira 180 para configurar o PuTTY para enviar dados keepalive a cada 3 minutos.
4. No painel Categoria, expanda Conexão, expanda SSH e selecione Auth. Completar o seguinte:
  - a. Escolha Navegar.
  - b. Selecione o arquivo .ppk gerado para seu par de chaves e escolha Open (Abrir).
  - c. (Opcional) Se você planeja iniciar esta sessão novamente depois, pode salvar as informações para uso futuro. Selecione Category (Categoria), escolha Session (Sessão), insira um nome para a sessão em Saved Sessions (Sessões salvas) e selecione Save (Salvar).
  - d. Escolha Open.
5. Se essa for a primeira vez você se conectou a esta instância, o PuTTY exibirá uma caixa de diálogo de alerta de segurança perguntando se você confia no host ao qual está se conectando.
  - a. (Opcional) Verifique se a impressão digital na caixa de diálogo do alerta de segurança corresponde à impressão digital que você obteve anteriormente em [\(Opcional\) Obter a impressão digital da instância \(p. 537\)](#). Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
  - b. Escolha Sim. Uma janela se abrirá e você estará conectado à sua instância.

#### Note

Se você especificou uma senha quando você converteu sua chave privada em formato PuTTY você deve fornecer essa senha quando você efetuar o login na instância.

Se você receber um erro ao tentar se conectar à instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#).

## Transferir arquivos da sua instância do Linux usando o cliente PuTTY Secure Copy

O cliente PuTTY Secure Copy (PSCP) é uma ferramenta de linha de comando que você pode usar para transferir arquivos entre seu computador Windows e sua instância do Linux. Se você preferir uma interface gráfica de usuário (GUI), pode usar uma ferramenta de GUI de uso aberto chamada WinSCP. Para obter mais informações, consulte [Transferir arquivos uma sua instância do Linux usando WinSCP \(p. 555\)](#).

Para usar o PSCP, você precisar da chave privada gerada em [Converta a chave privada usando o PuTTYgen \(p. 552\)](#). Você também precisa do nome DNS público da instância do Linux ou do endereço IPv6 se a instância tiver um.

O exemplo a seguir transfere o arquivo `Sample_file.txt` da unidade C:\ em um computador Windows para o diretório inicial `my-instance-user-name` em uma instância do Amazon Linux. Para transferir um arquivo, use um dos comandos a seguir.

- (DNS Público) Para transferir um arquivo usando o nome DNS público da instância, insira o comando a seguir.

```
pscp -i C:\\path\\my-key-pair.ppk C:\\path\\Sample_file.txt my-instance-user-name@my-instance-public-dns-name:/home/my-instance-user-name/Sample_file.txt
```

- (IPv6) Como alternativa, se a instância tiver um endereço IPv6, para transferir um arquivo usando o endereço IPv6 da instância, insira o comando a seguir. O endereço IPv6 deve estar entre colchetes ([ ]).

```
pscp -i C:\\path\\my-key-pair.ppk C:\\path\\Sample_file.txt my-instance-user-name@[my-instance-IPv6-address]:/home/my-instance-user-name/Sample_file.txt
```

## Transferir arquivos uma sua instância do Linux usando WinSCP

WinSCP é um gerenciador de arquivos baseado em GUI para Windows que permite que você carregue e transfira arquivos a um computador remoto usando os protocolos SFTP, SCP, FTP e FTPS. O WinSCP permite que você arraste e solte arquivos do computador Windows para a instância do Linux ou sincronize estruturas inteiras de diretório entre os dois sistemas.

### Requirements

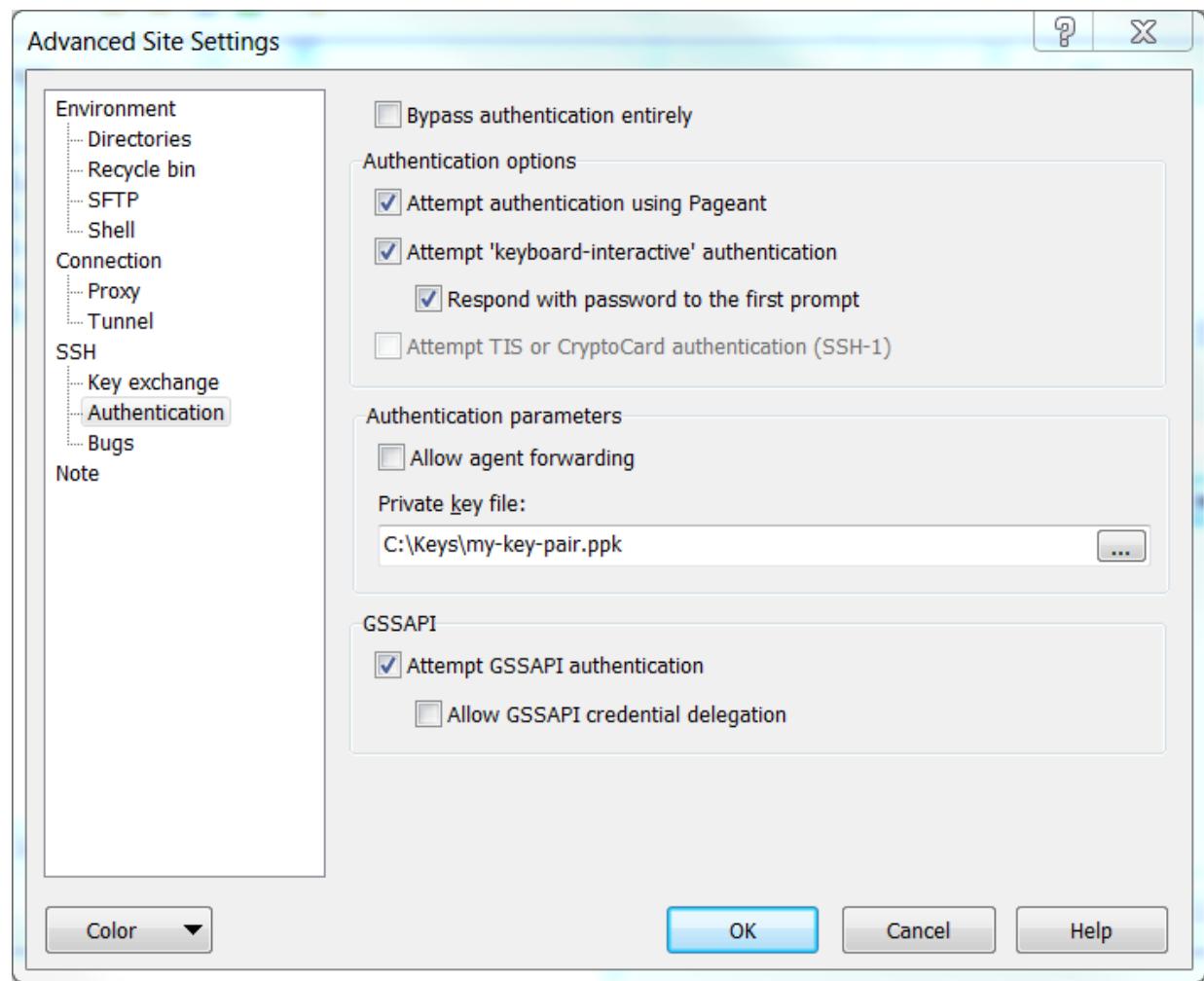
- É necessário ter a chave privada gerada no [Converta a chave privada usando o PuTTYgen \(p. 552\)](#).
- Também é necessário ter o nome DNS público da instância do Linux.
- Sua instância do Linux deve ter `scp` instalado. Para alguns sistemas operacionais, instale o pacote `openssh-clients`. Para outros, como a AMI otimizada para o Amazon ECS, instale o pacote `scp`. Verifique a documentação da sua distribuição do Linux.

### Como se conectar à instância usando WinSCP

1. Faça download e instale WinSCP em <http://winscp.net/eng/download.php>. Para a maioria dos usuários, as opções de instalação padrão são OK.
2. Inicie o WinSCP.
3. Na tela de Login do WinSCP, em Nome do host, insira uma das seguintes opções:
  - (DNS público ou endereço IPv4) Para fazer login usando o nome DNS público ou o endereço IPv4 público da instância, insira o nome DNS público ou o endereço IPv4 público da instância.

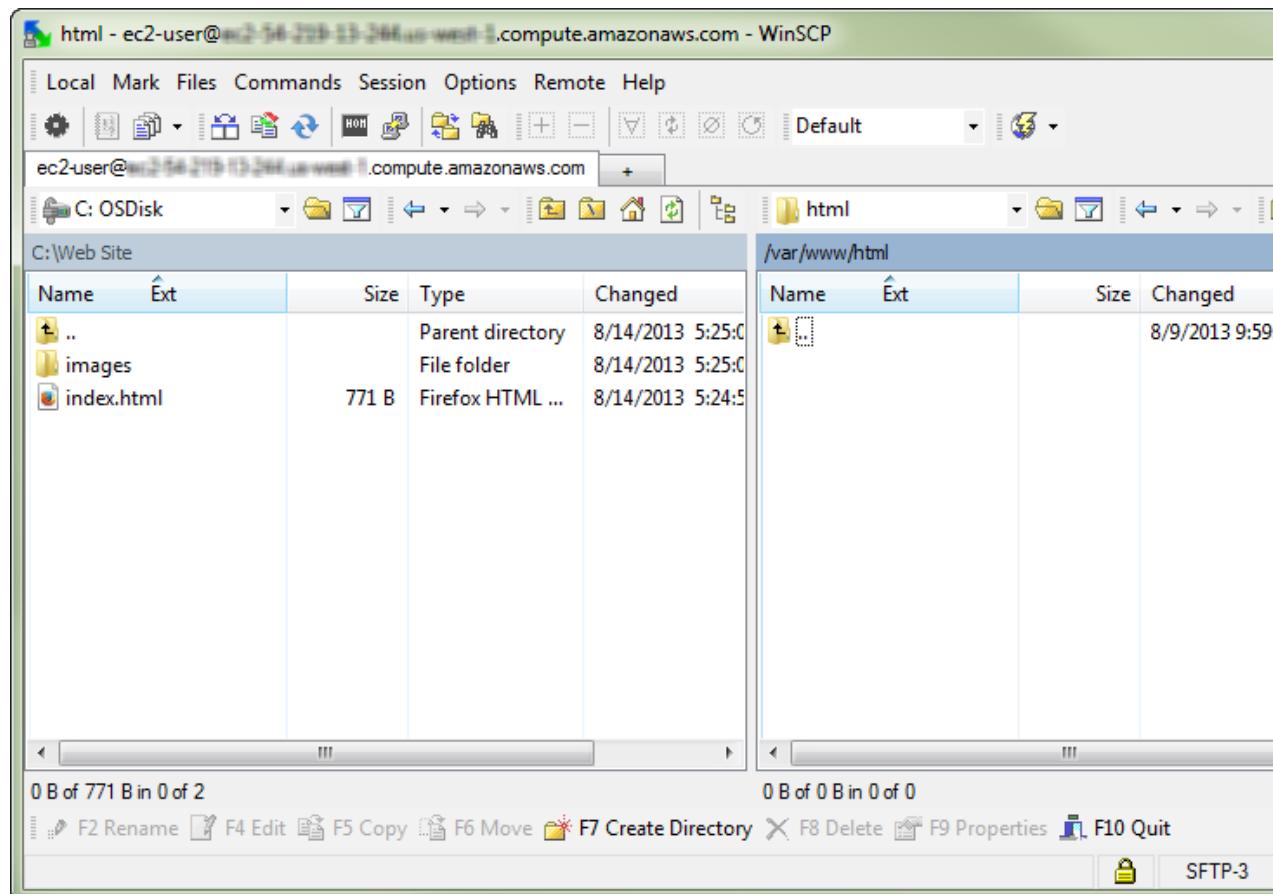
- (IPv6) Como alternativa, se a instância tiver um endereço IPv6, para fazer login usando o endereço IPv6 da instância, insira o endereço IPv6 para a instância.
4. Para Nome de usuário, insira o nome de usuário padrão para sua AMI.
    - Para o Amazon Linux 2 ou a AMI do Amazon Linux, o nome do usuário é `ec2-user`.
    - Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
    - Para uma AMI do Ubuntu, o nome do usuário é `admin`.
    - Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
    - Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.
    - Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.
    - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
    - Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
    - Para uma AMI do Bitnami, o nome do usuário é `bitnami`.
    - Caso contrário, verifique com o provedor da AMI.
  5. Especifique a chave privada para sua instância. Para Chave privada, insira o caminho a sua chave privada ou escolha o botão "..." para buscar pelo arquivo. Para abrir as configurações avançadas do site, em busca de novas versões do WinSCP, selecione Advanced (Avançado). Para localizar a configuração dePrivate key file (Arquivo de chave privada), em SSH, selecione Authentication (Autenticação).

Aqui está uma captura de tela do WinSCP versão 5.9.4:



O WinSCP exige um arquivo de chave privada do PuTTY (.ppk). Você pode converter um arquivo de chave de segurança .pem para o formato .ppk usando PuTTYgen. Para obter mais informações, consulte [Converta a chave privada usando o PuTTYgen \(p. 552\)](#).

6. (Opcional) No painel à esquerda, selecione Directories (Diretórios). Para Remote directory (Diretório remoto), informe o caminho para o diretório ao qual adicionar arquivos. Para abrir as configurações avançadas do site, em busca de novas versões do WinSCP, selecione Advanced (Avançado). Para encontrar a configuração Remote directory (Diretório remoto), em Environment (Ambiente), selecione Directories (Diretórios).
7. Escolha Login (Fazer login). Para adicionar a impressão digital do host, selecione Yes (Sim).



- Após a conexão ser estabelecida, na janela de conexão, sua instância do Linux está à direita e sua máquina local está à esquerda. É possível arrastar e soltar arquivos entre o sistema de arquivos remoto e a máquina local. Para obter mais informações sobre WinSCP, consulte a documentação do projeto em <http://winscp.net/eng/docs/start>.

Se você receber um erro indicando não ser possível executar o SCP para iniciar a transferência, verifique se você instalou scp na instância do Linux.

## Conectar-se à instância do Linux no Windows usando o Subsistema Windows para Linux

Depois que iniciar sua instância, você poderá conectá-la e usá-la da forma como usaria um computador bem na sua frente.

As instruções a seguir explicam como você se conecta à sua instância usando uma distribuição o Linux no Subsistema do Windows para Linux (WSL). O WSL pode ser baixado gratuitamente e permite que você execute ferramentas de linha de comando diretamente no Windows, no desktop tradicional do Windows, sem as despesas gerais de uma máquina virtual.

Ao instalar o WSL, você pode usar um ambiente Linux nativo para se conectar às instâncias EC2 do Linux, em vez de usar o PuTTY ou o PuTTYgen. No ambiente Linux, é mais fácil conectar-se às instâncias do Linux porque ele oferece um cliente SSH nativo que você pode usar para se conectar a essas instâncias e alterar as permissões do arquivo de chave .pem. O console do Amazon EC2 fornece o comando SSH para você se conectar com a instância do Linux. Além disso, você pode obter uma saída mais detalhada

do comando SSH para solução de problemas. Para obter mais informações, consulte a [documentação do Subsistema do Windows para Linux](#).

#### Note

Ao instalar o WSL, todos os pré-requisitos e etapas são iguais aos descritos em [Conectar-se à instância do Linux usando SSH \(p. 538\)](#), e a experiência é exatamente igual a usar um Linux nativo.

Se você receber um erro ao tentar se conectar à instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#).

#### Sumário

- [Prerequisites \(p. 538\)](#)
- [Conectar-se à instância do Linux usando WSL \(p. 559\)](#)
- [Transferir arquivos para instâncias do Linux usando SCP \(p. 560\)](#)
- [Desinstalar o WSL \(p. 562\)](#)

## Prerequisites

Antes de você se conectar à sua instância do Linux, preencha os pré-requisitos a seguir.

### Verifique se a instância está pronta

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique se a instância passou nas verificações de status. É possível visualizar essas informações na coluna Status check (Verificação de status) na página Instances (Instâncias).

### Verifique os pré-requisitos gerais para se conectar à instância

Para localizar o nome DNS público ou o endereço IP da instância e o nome de usuário que você deve usar para se conectar à instância, consulte [Pré-requisitos gerais para conectar-se à instância \(p. 535\)](#).

Instale o Subsistema Windows para Linux (WSL) e uma distribuição do Linux no computador local

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.

### Cópia da chave privada do Windows para o WSL

Em uma janela de terminal do WSL, copie o arquivo .pem (para o par de chaves que você especificou ao executar a instância) do Windows para o WSL. Observe o caminho totalmente qualificado para o arquivo .pem no WSL, que você deve usar para se conectar à sua instância. Para obter informações sobre como especificar o caminho para o disco rígido do Windows, consulte [How do I access my C drive?](#). Para obter mais informações sobre pares de chaves e instâncias do Windows, consulte [Pares de chaves do Amazon EC2 e instâncias do Windows](#).

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

## Conectar-se à instância do Linux usando WSL

Use o procedimento a seguir para se conectar à sua instância do Linux usando o Subsistema do Windows para Linux (WSL). Se você receber um erro ao tentar se conectar à instância, consulte [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#).

## Para se conectar à sua instância usando SSH

1. Em uma janela do terminal, use o comando ssh para se conectar à instância. Especifique o caminho e o nome do arquivo da chave privada (.pem), o nome de usuário da instância e o nome DNS público ou o endereço IPv6 da instância. Para obter mais informações sobre como localizar a chave privada, o nome de usuário da instância e o nome DNS ou o endereço IPv6 de uma instância, consulte [Encontrar a chave privada e definir as permissões \(p. 537\)](#) e [Obter informações sobre a instância \(p. 535\)](#). Para se conectar à instância, use um dos comandos a seguir.
  - (DNS público) Para se conectar usando o nome DNS público da instância, insira o comando a seguir.

```
ssh -i /path/my-key-pair.pem my-instance-user-name@my-instance-public-dns-name
```

- (IPv6) Como alternativa, se a instância tiver um endereço IPv6, você poderá se conectar à instância usando seu endereço IPv6. Especifique o comando ssh com o caminho até o arquivo de chave privada (.pem), o nome de usuário apropriado e o endereço IPv6.

```
ssh -i /path/my-key-pair.pem my-instance-user-name@my-instance-IPv6-address
```

Você verá uma resposta como a seguinte:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'  
can't be established.  
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.  
Are you sure you want to continue connecting (yes/no)?
```

2. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve anteriormente em [\(Opcional\) Obter a impressão digital da instância \(p. 537\)](#). Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
3. Digite yes.

Você verá uma resposta como a seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)  
to the list of known hosts.
```

## Transferir arquivos para instâncias do Linux usando SCP

O protocolo de cópia segura (SCP) é uma das alternativas para transferir arquivos entre seu computador local e uma instância do Linux. Esta seção descreve como transferir arquivos com o SCP. O procedimento é semelhante ao procedimento de conexão a uma instância com o SSH.

### Prerequisites

- Verifique os pré-requisitos gerais para transferir arquivos à instância.

Os pré-requisitos gerais para transferir arquivos para uma instância são os mesmos que os pré-requisitos gerais para se conectar a uma instância. Para obter mais informações, consulte [Pré-requisitos gerais para conectar-se à instância \(p. 535\)](#).

- Instalação de um cliente SCP

A maioria dos computadores com Linux, Unix e Apple incluem um cliente SCP por padrão. Se seu não incluir, o projeto OpenSSH oferece implantação gráts do pacote completo das ferramentas SSH, inclusive um cliente SCP. Para obter mais informações, consulte <https://www.openssh.com>.

As etapas de procedimento a seguir guiam você pelo uso de SCP para transferir o arquivo. Se você já tiver se conectado à instância com o SSH e tiver verificado suas impressões digitais, você poderá começar com a etapa que contém o comando SCP (etapa 4).

#### Para usar o SCP para transferir um arquivo

1. Transfira um arquivo para sua instância usando o nome DNS público da instância. Por exemplo, se o nome do arquivo de chave privada for `my-key-pair`, o arquivo a transferir for `SampleFile.txt`, o nome do usuário for `my-instance-user-name` e o nome DNS público da instância for `my-instance-public-dns-name` ou o endereço IPv6 for `my-instance-IPv6-address`, use os comandos a seguir para copiar o arquivo para o diretório inicial `my-instance-user-name`.
  - (DNS Público) Para transferir um arquivo usando o nome DNS público da instância, insira o comando a seguir.

```
scp -i /path/my-key-pair.pem /path/SampleFile.txt my-instance-user-name@my-instance-public-dns-name:-
```

- (IPv6) Como alternativa, se a instância tiver um endereço IPv6, você poderá transferir um arquivo usando o endereço IPv6 da instância. O endereço IPv6 deve vir entre colchetes ([ ]), que devem ser recuados (\).

```
scp -i /path/my-key-pair.pem /path/SampleFile.txt my-instance-user-name@[my-instance-IPv6-address]\:-
```

Você verá uma resposta como a seguinte:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)' can't be established.  
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.  
Are you sure you want to continue connecting (yes/no)?
```

2. (Opcional) Verifique se a impressão digital no alerta de segurança corresponde à impressão digital que você obteve anteriormente em [\(Opcional\) Obter a impressão digital da instância \(p. 537\)](#). Caso essas impressões digitais não correspondam, alguém pode estar tentando um ataque "man-in-the-middle". Se corresponderem, continue para a próxima etapa.
3. Digite **yes**.

Você verá uma resposta como a seguinte:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)  
to the list of known hosts.  
Sending file modes: C0644 20 SampleFile.txt  
Sink: C0644 20 SampleFile.txt  
SampleFile.txt 100% 20 0.0KB/s 00:00
```

Se você receber o erro "bash: scp: command not found", deverá primeiro instalar scp na sua instância do Linux. Para alguns sistemas operacionais, isso está localizado no pacote `openssh-clients`. Para variantes do Amazon Linux, como a Amazon ECS otimizada por AMI, use o comando para instalar o scp:

```
[ec2-user ~]$ sudo yum install -y openssh-clients
```

4. Para transferir arquivos na outra direção (de uma instância do Amazon EC2 para o computador local), basta inverter a ordem dos parâmetros do host. Por exemplo, para transferir o arquivo `SampleFile.txt` da instância do EC2 de volta ao diretório inicial no computador local como `SampleFile2.txt`, use um dos comandos a seguir no computador local.

- (DNS Público) Para transferir um arquivo usando o nome DNS público da instância, insira o comando a seguir.

```
scp -i /path/my-key-pair.pem my-instance-user-name@ec2-198-51-100-1.compute-1.amazonaws.com:~/SampleFile.txt ~/SampleFile2.txt
```

- (IPv6) Como alternativa, se a instância tiver um endereço IPv6, para transferir arquivos na outra direção usando o endereço IPv6 da instância, insira o comando a seguir.

```
scp -i /path/my-key-pair.pem my-instance-user-name@[2001:db8:1234:1a00:9691:9503:25ad:1761]:~/SampleFile.txt ~/SampleFile2.txt
```

## Desinstalar o WSL

Para obter informações sobre como desinstalar o Subsistema Windows para Linux, consulte [Como desinstalar o WSL Distribution?](#).

## Conectar-se à instância do Linux usando o Gerenciador de sessões

O gerenciador de sessões é um recurso totalmente gerenciado do AWS Systems Manager que permite 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 bash como faria por meio de 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 e instruções, consulte [Conceitos básicos do Gerenciador de sessões](#).

Como se conectar a uma instância do Linux usando o Gerenciador de sessões com 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 Connect (Conectar).
4. Em Connection method (Método de conexão), escolha Session Manager (Gerenciador de sessões).
5. Selecione Conectar.

### Troubleshooting

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, 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).

## 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 \(p. 563\)](#).

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 \(p. 587\)](#). Se você preferir hibernar a instância, consulte [Hibernar a instância do Windows sob demanda ou reservada \(p. 566\)](#). Para obter mais informações, consulte [Diferenças entre reinicialização, interrupção, hibernação e encerramento \(p. 507\)](#).

## Tópicos

- [Overview \(p. 563\)](#)
- [O que acontece quando você interrompe uma instância \(p. 564\)](#)
- [Interromper e iniciar suas instâncias \(p. 564\)](#)
- [Modificar uma instância interrompida \(p. 566\)](#)
- [Solução de problemas na interrupção da instância \(p. 566\)](#)

## Overview

Você só pode interromper uma instância com Amazon EBS. Para verificar o tipo de dispositivo raiz da sua instância, descreva-a e verifique se o tipo de dispositivo de seu volume do dispositivo raiz é `ebs` (instância com Amazon EBS) ou `instance store` (instância com armazenamento de instâncias). Para obter mais informações, consulte [Determinar o tipo de dispositivo raiz da AMI \(p. 76\)](#).

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 \(p. 1100\)](#).
- 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 [Configuração de uma instância do Windows usando o serviço EC2Config](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

- 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 \(p. 1109\)](#).

Para obter mais informações, consulte [Diferenças entre reinicialização, interrupção, hibernação e encerramento \(p. 507\)](#).

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 (por exemplo, usando os comandos `shutdown` ou `poweroff`), 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 \(p. 591\)](#).

Usar o comando `halt` em uma instância não inicia um desligamento. Se ele for usado, a instância não será encerrada. Em vez disso, ele colocará a CPU em `HLT` e a instância permanecerá em execução.

## 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 \(p. 566\)](#).
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 \(p. 566\)](#).
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 \(p. 327\)](#).
- Para alterar os dados do usuário para sua instância, consulte [Trabalhar com dados do usuário da instância \(p. 664\)](#).
- Para habilitar ou desabilitar a otimização do EBS para sua instância, consulte [Modifying EBS–Optimization \(Modificar a otimização do EBS\) \(p. 1459\)](#).
- 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 \(p. 1538\)](#). 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 \(p. 1583\)](#).

## Hibernar a instância do Windows 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 \(p. 575\)](#) e atender aos [pré-requisitos de hibernação \(p. 568\)](#).

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 \(p. 562\)](#) 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 \(p. 587\)](#).

#### Note

Para obter informações sobre como usar a hibernação em instâncias do Windows, consulte [Hibernar a instância do Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

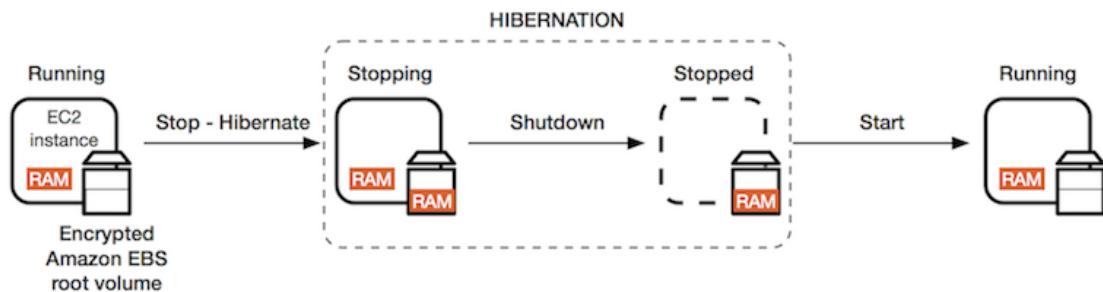
Para obter informações sobre o Instâncias spot em hibernação, consulte [Hibernar Instâncias spot interrompida \(p. 429\)](#).

#### Tópicos

- [Visão geral da hibernação \(p. 567\)](#)
- [Pré-requisitos de hibernação \(p. 568\)](#)
- [Limitations \(p. 571\)](#)
- [Configurar uma AMI existente para oferecer suporte à hibernação \(p. 571\)](#)
- [Habilitar a hibernação para uma instância \(p. 575\)](#)
- [Desabilitar o KASLR em uma instância \(apenas Ubuntu\) \(p. 578\)](#)
- [Hibernar uma instância \(p. 579\)](#)
- [Iniciar um instância em hibernação \(p. 581\)](#)
- [Solucionar problemas de hibernação \(p. 582\)](#)

## 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 \(p. 1100\)](#).
- 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 \(p. 1109\)](#).

Para obter informações sobre como a hibernação difere da reinicialização, da interrupção e do encerramento, consulte [Diferenças entre reinicialização, interrupção, hibernação e encerramento \(p. 507\)](#).

## Pré-requisitos de hibernação

Para hibernar uma instância sob demanda ou Instância reservada, os seguintes pré-requisitos devem estar implementados:

- [AMIs compatíveis Linux \(p. 568\)](#)
- [Famílias de instâncias compatíveis \(p. 569\)](#)
- [Tamanho da instância \(p. 570\)](#)
- [Tamanho da instância RAM \(p. 570\)](#)
- [Tipo do volume de raiz \(p. 570\)](#)
- [Tamanho do volume raiz do EBS \(p. 570\)](#)
- [Tipos de volume EBS compatíveis \(p. 570\)](#)
- [Criptografia do volume raiz EBS \(p. 570\)](#)
- [Ativar hibernação no lançamento \(p. 571\)](#)
- [Opções de compra \(p. 571\)](#)

## AMIs compatíveis Linux

Deve ser uma AMI do HVM que ofereça suporte à hibernação:

AMI	Xen -supported instance families only	Nitro - supported instance families only
AMI do Amazon Linux 2 lançada em 29/08/2019 ou posterior	Compatível	Compatível
AMI do Amazon Linux 2018.03 lançada em 16/11/2018 ou posterior	Compatível	Compatível
CentOS versão 8 AMI* ( <a href="#">configuração adicional (p. 573)</a> necessária)	Sem suporte	Compatível
Fedora versão 34 ou posterior AMI* ( <a href="#">configuração adicional (p. 573)</a> necessária)	Sem suporte	Compatível
Red Hat Enterprise Linux (RHEL) 8 AMI* ( <a href="#">configuração adicional (p. 574)</a> necessária)	Sem suporte	Compatível
AMI do Ubuntu 18.04 LTS - Bionic liberada com o número de série 20190722.1 ou posterior †	Compatível	Compatível
Ubuntu 16.04 LTS - Xenial AMI † ( <a href="#">configuração adicional (p. 575)</a> necessária)	Compatível	Compatível

\* Para CentOS, Fedora e Red Hat Enterprise Linux, a hibernação é possível apenas em instâncias baseadas em Nitro.

† Recomendamos desabilitar o KASLR em instâncias com o Ubuntu 18.04 LTS - Bionic e Ubuntu 16.04 LTS - Xenial. Para obter mais informações, consulte [Desabilitar o KASLR em uma instância \(apenas Ubuntu\) \(p. 578\)](#).

Para configurar sua AMI para oferecer suporte à hibernação, consulte [Configurar uma AMI existente para oferecer suporte à hibernação \(p. 571\)](#).

O suporte para outras versões do Ubuntu e outros sistemas operacionais será disponibilizado em breve.

Para obter informações sobre as AMIs Windows compatíveis, consulte [AMIs compatíveis com o Windows no Manual do usuário do Amazon EC2 para instâncias do Windows](#).

## 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 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.

```
$ 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

Deve ter menos de 150 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 \(p. 1253\)](#).

## 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 \(p. 1421\)](#).

- 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 \(p. 163\)](#).
- 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 \(p. 167\)](#) e [Copiar um AMI \(p. 145\)](#).

## 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 \(p. 575\)](#).

## 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 \(p. 429\)](#).

## 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 150 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.

## Configurar uma AMI existente para oferecer suporte à hibernação

As seguintes AMIs suportam hibernação, mas, para hibernar uma instância que foi iniciada com uma dessas AMIs, é necessária uma configuração adicional para que você possa colocar a instância em hibernação.

Configurações adicionais são necessárias para:

- [Amazon Linux 2 lançado antes de 29/08/2019 \(p. 572\)](#)
- [Amazon Linux lançado antes de 16/11/2018 \(p. 572\)](#)
- [CentOS versão 8 ou posterior \(p. 573\)](#)

- [Fedora versão 34 ou posterior \(p. 573\)](#)
- [Red Hat Enterprise Linux versão 8 ou posterior \(p. 574\)](#)
- [Ubuntu 18.04 - Bionic lançada antes do número de série 20190722.1 \(p. 574\)](#)
- [Ubuntu 16.04 - Xenial \(p. 575\)](#)

Para obter mais informações, consulte [Atualizar o software da instância na instância do Amazon Linux \(p. 597\)](#).

Nenhuma configuração adicional é necessária para as AMIs a seguir, porque elas já estão configuradas para suportar hibernação:

- AMI do Amazon Linux 2 lançada em 29/08/2019 ou posterior
- AMI do Amazon Linux 2018.03 lançada em 16/11/2018 ou posterior
- AMI do Ubuntu 18.04 LTS - Bionic lançada com o número de série 20190722.1 ou posterior

## Amazon Linux 2 lançado antes de 29/08/2019

Como configurar uma AMI do Amazon Linux 2 lançada antes de 29/08/2019 para suportar hibernação

1. Atualize o kernel para 4.14.138-114.102 ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o pacote ec2-hibinit-agent dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Reinicie a instância.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme se a versão do kernel está atualizada para 4.14.138-114.102 ou posterior.

```
[ec2-user ~]$ uname -a
```

5. Interrompa a instância e crie uma AMI. Para obter mais informações, consulte [Criar uma AMI do Linux a partir de uma instância \(p. 108\)](#).

## Amazon Linux lançado antes de 16/11/2018

Para configurar uma AMI do Amazon Linux lançada antes de 16/11/2018 para oferecer suporte à hibernação

1. Atualize o kernel para 4.14.77-70.59 ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o pacote ec2-hibinit-agent dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Reinicie a instância.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme se a versão do kernel está atualizada para 4.14.77-70.59 ou maior.

```
[ec2-user ~]$ uname -a
```

5. Interrompa a instância e crie uma AMI. Para obter mais informações, consulte [Criar uma AMI do Linux a partir de uma instância \(p. 108\)](#).

## CentOS versão 8 ou posterior

Para configurar uma AMI do CentOS versão 8 ou posterior para suportar hibernação

1. Atualize o kernel para 4.18.0-305.7.1.el8\_4.x86\_64 ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o repositório Fedora Extra Packages for Enterprise Linux (EPEL).

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Instale o pacote ec2-hibinit-agent dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Habilite o agente de hibernação para iniciar na inicialização.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

6. Confirme se a versão do kernel está atualizada para 4.18.0-305.7.1.el8\_4.x86\_64 ou posterior.

```
[ec2-user ~]$ uname -a
```

## Fedora versão 34 ou posterior

Para configurar uma AMI do Fedora versão 34 ou posterior para suportar hibernação

1. Atualize o kernel para 5.12.10-300.fc34.x86\_64 ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o pacote ec2-hibinit-agent dos repositórios.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Habilite o agente de hibernação para iniciar na inicialização.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

5. Confirme se a versão do kernel está atualizada para 5.12.10-300.fc34.x86\_64 ou posterior.

```
[ec2-user ~]$ uname -a
```

## Red Hat Enterprise Linux versão 8 ou posterior

Para configurar uma AMI do Red Hat Enterprise Linux 8 para suportar hibernação

1. Atualize o kernel para 4.18.0-305.7.1.el8\_4.x86\_64 ou posterior.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Instale o repositório Fedora Extra Packages for Enterprise Linux (EPEL).

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Instale o pacote ec2-hibinit-agent dos repositórios.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Habilite o agente de hibernação para iniciar na inicialização.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

6. Confirme se a versão do kernel está atualizada para 4.18.0-305.7.1.el8\_4.x86\_64 ou posterior.

```
[ec2-user ~]$ uname -a
```

## Ubuntu 18.04 - Bionic lançada antes do número de série 20190722.1

Para configurar uma AMI do Ubuntu 18.04 LTS lançada antes do número de série 20190722.1 para suportar hibernação

1. Atualize o kernel para 4.15.0-1044 ou posterior.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Instale o pacote ec2-hibinit-agent dos repositórios.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme se a versão do kernel está atualizada para 4.15.0-1044 ou posterior.

```
[ec2-user ~]$ uname -a
```

## Ubuntu 16.04 - Xenial

Para configurar o Ubuntu 16.04 LTS para ser compatível com a hibernação, é necessário instalar o pacote do kernel linux-aws-hwe versão 4.15.0-1058-aws ou posterior e o agente ec2-hibint.

Como configurar uma AMI do Ubuntu 16.04 LTS para que seja compatível com a hibernação

1. Atualize o kernel para 4.15.0-1058-aws ou posterior.

```
[ec2-user ~]$ sudo apt update  
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

### Note

O pacote do kernel `linux-aws-hwe` é totalmente compatível com o Canonical. O pacote continuará a receber atualizações regulares até que o suporte padrão para o Ubuntu 16.04 LTS termine em abril de 2021 e receberá atualizações de segurança adicionais até que o suporte de Manutenção de segurança estendida termine em 2024. Para obter mais informações, consulte [Amazon EC2 Hibernation for Ubuntu 16.04 LTS now available](#) no blog do Canonical Ubuntu.

2. Instale o pacote `ec2-hibinit-agent` dos repositórios.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

4. Confirme se a versão do kernel está atualizada para 4.15.0-1058-aws ou posterior.

```
[ec2-user ~]$ uname -a
```

## 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. \(p. 510\)](#).

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 \(p. 568\)](#).
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 \(p. 568\)](#).
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 \(p. 568\)](#).

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. \(p. 510\)](#).

## 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.

## Desabilitar o KASLR em uma instância (apenas Ubuntu)

Para executar a hibernação em uma instância recém-executada com o Ubuntu 16.04 LTS - Xenial ou o Ubuntu 18.04 -Bionic, liberado com o número serial 20190722,1 ou posterior, recomendamos desabilitar o KASLR (Kernel Address Space Layout Randomization). No Ubuntu 16.04 LTS ou no Ubuntu 18.04 LTS, o KASLR é habilitado por padrão. O KASLR é um recurso de segurança do kernel padrão do Linux que ajuda a mitigar as ramificações de e a exposição e às vulnerabilidades de acesso à memória ainda não descobertas por randomização do valor base do endereço do kernel. Com o KASLR habilitado, há uma possibilidade de a instância não ser retomada depois de ter estado em hibernação.

Para saber mais sobre o KASLR, consulte [Recursos do Ubuntu](#).

Para desabilitar o KASLR em uma instância executada com o Ubuntu

1. Conecte-se à sua instância usando SSH. Para obter mais informações, consulte [Conectar-se à instância do Linux usando SSH \(p. 538\)](#).

2. Abra o arquivo `/etc/default/grub.d/50-cloudimg-settings.cfg` com seu editor de preferência. Edite a linha `GRUB_CMDLINE_LINUX_DEFAULT` para anexar a opção `nokaslr` no final, conforme mostrado no exemplo a seguir.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0 nvme_core.io_timeout=4294967295
nokaslr"
```

3. Salve o arquivo e saia do editor.
4. Execute o comando a seguir para recompilar a configuração do grub.

```
[ec2-user ~]$ sudo update-grub
```

5. Reinicialize a instância.

```
[ec2-user ~]$ sudo reboot
```

6. Execute o seguinte comando para confirmar que `nokaslr` foi adicionado.

```
[ec2-user ~]$ cat /proc/cmdline
```

A saída do comando deve incluir a opção `nokaslr`.

## Hibernar uma instância

É possível hibernar uma instância se ela estiver [habilitada para hibernação \(p. 575\)](#) e atender aos [pré-requisitos de hibernação \(p. 568\)](#). 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 \(p. 568\)](#).
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 \(p. 568\)](#).

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 \(p. 842\)](#) 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 \(p. 842\)](#) 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 dois 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.

Verifique o log do sistema da instância e procure as mensagens relacionadas à hibernação. Para acessar o log do sistema, [conecte-se \(p. 535\)](#) à instância ou use o comando [get-console-output](#). Localize as linhas do log no `hibinit-agent`. 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:  
`hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Se a última linha do log no `hibinit-agent` for `hibinit-agent: Running: swapoff /swap`, a hibernação foi 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 \(p. 568\)](#). Se tiver usado sua própria AMI, verifique se você seguiu as instruções para [Configurar uma AMI existente para oferecer suporte à hibernação \(p. 571\)](#).

### 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 \(p. 1583\)](#).

## 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 \(p. 848\)](#).

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 reiniciar sua instância também criará um registro de API de quando a instância foi reinicializada.

### New console

#### Para reiniciar 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 reiniciar 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 reiniciar 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 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. Iniciar a instância interrompida migra-a para o novo hardware.
- 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 sobre os tipos de eventos de instância, consulte [Eventos programados para instâncias \(p. 848\)](#).

### Tópicos

- [Identificar instâncias programadas para desativação \(p. 584\)](#)
- [Ações a serem executadas para instâncias baseadas em EBS programadas para desativação \(p. 585\)](#)
- [Ações a serem executadas para instâncias com armazenamento de instâncias programadas para desativação \(p. 586\)](#)

## 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 \(p. 584\)](#)
- [Identificação do console \(p. 584\)](#)

## 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.

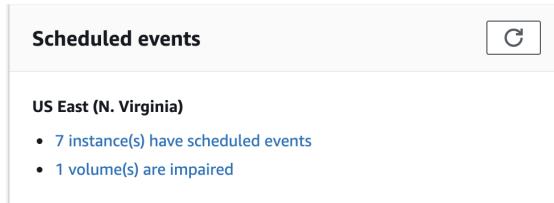
O e-mail é enviado ao titular da conta principal e ao contato de operações. Para obter mais informações, consulte [Adding, changing, or removing alternate contacts \(Adicionar, alterar ou remover contatos alternativos\)](#) no AWS Billing and Cost Management User Guide (Manual do usuário do AWS Billing 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 baseadas em EBS 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.

Se você não souber ao certo se sua instância tem suporte do EBS ou do armazenamento de instâncias, consulte [Determinar o tipo de dispositivo raiz da instância \(p. 1524\)](#).

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 \(p. 535\)](#) 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 \(p. 562\)](#). 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 \(p. 562\)](#) para recuperar sua instância.
- Se preferir [encerrar \(p. 587\)](#) 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 Linux baseada em Amazon EBS \(p. 107\)](#).

#### 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. \(p. 510\)](#).

## Ações a serem executadas para instâncias com armazenamento de 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.

#### Warning

Se a sua instância baseada em armazenamento de instâncias passar de sua data de desativação, ela será encerrada e você não poderá recuperar a instância nem os dados que foram armazenados nela. Independentemente do dispositivo raiz de sua instância, os dados em volumes de armazenamento de instâncias são perdidos quando a instância é desativada, mesmo que os volumes estejam anexados a uma instância baseada no EBS.

#### 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 \(p. 535\)](#) ou fazendo ping na instância.
- Se sua instância estiver inacessível, é provável que haja muito pouco que possa ser feito para recuperá-la. Para obter mais informações, consulte [Solucionar problemas de uma instância não acessível \(p. 1609\)](#). A AWS encerrará a instância na data de desativação programada, portanto, para uma instância inacessível, você pode [encerrar \(p. 587\)](#) a instância por conta própria.

#### Execute uma instância de substituição

Crie uma AMI com armazenamento de instâncias a partir da sua instância usando as ferramentas da AMI, conforme descrito em [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#). 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. \(p. 510\)](#).

#### Converta sua instância em uma instância baseada em EBS

Transfira seus dados para um volume do EBS, obtenha um snapshot do volume e crie a AMI a partir do snapshot. Você pode executar uma instância de substituição a partir da nova AMI. Para obter mais informações, consulte [Converter de uma AMI com armazenamento de instâncias em uma AMI com Amazon EBS \(p. 124\)](#).

## 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 \(p. 562\)](#) ou [Hibernar a instância do Windows sob demanda ou reservada \(p. 566\)](#). Para obter mais informações, consulte [Diferenças entre reinicialização, interrupção, hibernação e encerramento \(p. 507\)](#).

### Tópicos

- [Encerramento de instância \(p. 587\)](#)
- [Terminar várias instâncias com proteção contra término entre zonas de disponibilidade \(p. 588\)](#)
- [O que acontece quando você encerra uma instância \(p. 588\)](#)
- [Como encerrar uma instância \(p. 589\)](#)
- [Habilitar a proteção contra encerramento \(p. 589\)](#)
- [Alterar o comportamento de desligamento iniciado da instância \(p. 591\)](#)
- [Preservar volumes do Amazon EBS no encerramento da instância \(p. 591\)](#)
- [Soluç�ao de problemas de encerramento da instância \(p. 593\)](#)

## 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 \(p. 591\)](#).

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 \(p. 589\)](#).

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 \(p. 591\)](#).

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 HLT 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 acidentalmente 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 `InstanceInitiatedShutdownBehavior` é definido. Para obter mais informações, consulte [Alterar o comportamento de desligamento iniciado da instância \(p. 591\)](#).

#### 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 \(p. 427\)](#).

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 \(p. 1277\)](#), 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 \(p. 1302\)](#).

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 \(p. 1538\)](#).

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 \(p. 592\)](#)
- [Alterar o volume raiz a ser mantido na execução usando a linha de comando \(p. 592\)](#)
- [Alterar o volume raiz de uma instância em execução a ser mantido usando a linha de comando \(p. 593\)](#)

## 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  
    }  
  }  
]
```

## Solucionar problemas de encerramento da instância

Se você encerrar a instância e outra instância for iniciada, provavelmente você configurou a escalabilidade automática por meio de um recurso como o Frota do EC2 ou o Amazon EC2 Auto Scaling.

Se a instância permanecer no estado `shutting-down` por mais tempo do que o normal, ela será removida (encerrada) por processos automatizados no serviço do Amazon EC2. Para obter mais informações, consulte [Encerramento atrasado da instância \(p. 1586\)](#).

## 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 reterá 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 \(p. 594\)](#)
- [Crie um alarme Amazon CloudWatch para recuperar uma instância \(p. 594\)](#)
- [Solucionar problemas de falhas de recuperação da instância \(p. 594\)](#)

## Requirements

A ação de recuperação é compatível somente nas instâncias com as seguintes características:

- Usa um dos seguintes tipos de instância: A1, C3, C4, C5, C5a, C5n, C6g, C6gn, Inf1, M3, M4, M5, M5a, M5n, M5zn, M6g, M6i, P3, R3, R4, R5, R5a, R5b, R5n, R6g, T2, T3, T3a, T4g, 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 \(p. 904\)](#).

## 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 \(p. 562\)](#).

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 Amazon Linux

Após executar e se conectar à sua instância do Amazon Linux com êxito, você pode fazer alterações nela. Há muitas maneiras diferentes de configurar uma instância para atender às necessidades de uma aplicação específica. A seguir, temos algumas tarefas comuns para ajudá-lo a começar.

### Tópicos

- [Cenários de configuração comuns \(p. 595\)](#)
- [Gerenciar software na instância do Amazon Linux \(p. 596\)](#)
- [Gerenciar contas de usuário na instância do Amazon Linux \(p. 602\)](#)
- [Controle do estado do processo para a instância do EC2 \(p. 604\)](#)
- [Definir o horário da sua instância do Linux \(p. 610\)](#)
- [Otimizar as opções de CPU \(p. 616\)](#)
- [Alterar o nome do host da instância do Amazon Linux \(p. 637\)](#)
- [Configurar um DNS dinâmico na instância do Amazon Linux \(p. 640\)](#)
- [Executar comandos na instância do Linux na inicialização \(p. 642\)](#)
- [Metadados da instância e dados do usuário \(p. 649\)](#)

## Cenários de configuração comuns

A distribuição básica do Amazon Linux contém vários pacotes e utilitários de software que são necessários para operações básicas de servidor. Contudo, muito mais pacotes de software estão disponíveis em vários repositórios de software e ainda mais pacotes estão disponíveis para criação a partir do código-fonte. Para obter mais informações sobre instalação e criação de software desses locais, consulte [Gerenciar software na instância do Amazon Linux \(p. 596\)](#).

As instâncias do Amazon Linux vêm pré-configuradas com uma conta `ec2-user`, mas talvez você queira adicionar outras contas de usuário que não têm privilégios de superusuário. Para obter mais informações sobre como adicionar e remover contas de usuário, consulte [Gerenciar contas de usuário na instância do Amazon Linux \(p. 602\)](#).

A configuração de tempo padrão para instâncias do Amazon Linux usa o Amazon Time Sync Service para configurar a hora do sistema em uma instância. O fuso horário é UTC por padrão. Para obter mais

informações sobre como configurar o fuso horário de uma instância ou usar seu próprio servidor de tempo, consulte [Definir o horário da sua instância do Linux \(p. 610\)](#).

Se você tiver sua própria rede com um nome de domínio registrado, poderá alterar o nome do host de uma instância para que ela se identifique como parte do domínio. Você também pode alterar o prompt do sistema para mostrar um nome mais significativo sem alterar as configurações de nome de host.

Para obter mais informações, consulte [Alterar o nome do host da instância do Amazon Linux \(p. 637\)](#). Você pode configurar uma instância para usar um provedor de serviço DNS dinâmico. Para obter mais informações, consulte [Configurar um DNS dinâmico na instância do Amazon Linux \(p. 640\)](#).

Ao executar uma instância no Amazon EC2, você tem a opção de passar dados de usuário para a instância que podem ser usados para realizar tarefas de configuração comuns e até mesmo executar scripts após a inicialização da instância. Você pode passar dois tipos de dados de usuário para as diretivas de cloud-init do Amazon EC2: e os scripts de shell. Para obter mais informações, consulte [Executar comandos na instância do Linux na inicialização \(p. 642\)](#).

## Gerenciar software na instância do Amazon Linux

A distribuição básica do Amazon Linux contém vários pacotes e utilitários de software que são necessários para operações básicas de servidor. Muito mais pacotes de software estão disponíveis em vários repositórios de software e ainda mais pacotes estão disponíveis para criação a partir do código-fonte.

### Tópicos

- [Atualizar o software da instância na instância do Amazon Linux \(p. 597\)](#)
- [Adicionar repositórios em uma instância do Amazon Linux \(p. 598\)](#)
- [Encontrar pacotes de software em uma instância do Amazon Linux \(p. 599\)](#)
- [Instalar pacotes de software em uma instância do Amazon Linux \(p. 600\)](#)
- [Preparar-se para compilar software em uma instância do Amazon Linux \(p. 601\)](#)

É importante manter o software atualizado. Muitos pacotes em uma distribuição do Linux são atualizados frequentemente para corrigir erros, adicionar recursos e proteger contra exploits de segurança. Para obter mais informações, consulte [Atualizar o software da instância na instância do Amazon Linux \(p. 597\)](#).

Por padrão, as instâncias do Amazon Linux são executadas com os dois repositórios habilitados a seguir:

- Amazon Linux 2: `amzn2-core` e `amzn2extra-docker`
- Amazon Linux AMI: `amzn-main` e `amzn-updates`

Embora haja muitos pacotes disponíveis nesses repositórios que são atualizados pela Amazon Web Services, pode haver um pacote que você deseja instalar e que esteja contido em outro repositório. Para obter mais informações, consulte [Adicionar repositórios em uma instância do Amazon Linux \(p. 598\)](#). Para obter ajuda para localizar pacotes nos repositórios habilitados, consulte [Encontrar pacotes de software em uma instância do Amazon Linux \(p. 599\)](#). Para obter informações sobre como instalar uma instância do Amazon Linux, consulte [Instalar pacotes de software em uma instância do Amazon Linux \(p. 600\)](#).

Nem todo software está disponível em pacotes de software armazenados em repositórios; alguns devem ser compilados em uma instância a partir do código-fonte. Para obter mais informações, consulte [Preparar-se para compilar software em uma instância do Amazon Linux \(p. 601\)](#).

As instâncias do Amazon Linux gerenciam seu software usando o gerenciador de pacotes yum. O gerenciador de pacotes yum pode instalar, remover e atualizar software, bem como gerenciar todas as dependências para cada pacote. As distribuições do Linux baseadas em Debian, como Ubuntu, usam o

comando apt-get e o gerenciador de pacotes dpkg, logo, os exemplos de yum nas seções a seguir não se aplicam a essas distribuições.

## Atualizar o software da instância na instância do Amazon Linux

É importante manter o software atualizado. Muitos pacotes em uma distribuição do Linux são atualizados frequentemente para corrigir erros, adicionar recursos e proteger contra exploits de segurança. Quando você executar e se conectar a uma instância do Amazon Linux pela primeira vez, talvez veja uma mensagem solicitando que atualize os pacotes de software para fins de segurança. Esta seção mostra como atualizar todo um sistema ou apenas um único pacote.

### Important

Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

Para atualizar todos os pacotes em uma instância do Amazon Linux

1. (Opcional) Inicie uma sessão de screen em sua janela de shell. Às vezes, pode haver uma interrupção de rede que pode desconectar a conexão de SSH com sua instância. Se isso acontecer durante uma atualização longa de software, poderá deixar a instância em um estado recuperável, embora confuso. Uma sessão de screen permite que você continue executando a atualização mesmo se sua conexão for interrompida, e você poderá se reconectar à sessão posteriormente sem problemas.
  - a. Execute o comando screen para iniciar a sessão.

```
[ec2-user ~]$ screen
```

- b. Se a sessão for desconectada, se conecte novamente com sua instância e liste as telas disponíveis.

```
[ec2-user ~]$ screen -ls
There is a screen on:
    17793.pts-0.ip-12-34-56-78 (Detached)
    1 Socket in /var/run/screen/S-ec2-user.
```

- c. Reconecte a tela usando o comando screen -r e o ID de processo do comando anterior.

```
[ec2-user ~]$ screen -r 17793
```

- d. Quando terminar de usar screen, use o comando exit para fechar a sessão.

```
[ec2-user ~]$ exit
[screen is terminating]
```

2. Execute o comando yum update. Opcionalmente, você pode adicionar o sinalizador --security para aplicar apenas atualizações de segurança.

```
[ec2-user ~]$ sudo yum update
```

3. Revise os pacotes relacionados, digite y e pressione Enter para aceitar as atualizações. A atualização de todos os pacotes em um sistema pode levar vários minutos. A saída yum mostra o status da atualização durante sua execução.
  4. (Opcional) Reinicialize sua instância para garantir que você está usando os pacotes e as bibliotecas mais recentes de sua atualização. Atualizações de kernel não são carregadas até que uma reinicialização ocorra. Também é necessário reinicializar após atualizações de bibliotecas glibc. Para atualizações de pacotes que controlam serviços, pode ser suficiente reiniciar os serviços para

obter as atualizações, mas a reinicialização do sistema garante que todas as atualizações de pacotes e bibliotecas anteriores sejam concluídas.

Para atualizar um único pacote em uma instância do Amazon Linux

Use este procedimento para atualizar um único pacote (e suas dependências) e não o sistema inteiro.

1. Execute o comando yum update com o nome de pacote a ser atualizado.

```
[ec2-user ~]$ sudo yum update openssl
```

2. Revise as informações de pacotes listadas, digite **y** e pressione Enter para aceitar a atualização ou as atualizações. Às vezes, haverá mais de um pacote listado se houver dependências de pacotes que devem ser resolvidas. A saída yum mostra o status da atualização durante sua execução.
3. (Opcional) Reinicie sua instância para garantir que você está usando os pacotes e as bibliotecas mais recentes de sua atualização. Atualizações de kernel não são carregadas até que uma reinicialização ocorra. Também é necessário reiniciarizar após atualizações de bibliotecas glibc. Para atualizações de pacotes que controlam serviços, pode ser suficiente reiniciar os serviços para obter as atualizações, mas a reinicialização do sistema garante que todas as atualizações de pacotes e bibliotecas anteriores sejam concluídas.

## Adicionar repositórios em uma instância do Amazon Linux

Por padrão, as instâncias do Amazon Linux são executadas com os dois repositórios habilitados a seguir:

- Amazon Linux 2: `amzn2-core` e `amzn2extra-docker`
- Amazon Linux AMI: `amzn-main` e `amzn-updates`

Embora haja muitos pacotes disponíveis nesses repositórios que são atualizados pela Amazon Web Services, pode haver um pacote que você deseje instalar e que esteja contido em outro repositório.

### Important

Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

Para instalar um pacote de um repositório diferente com yum, você precisa adicionar as informações do repositório ao arquivo `/etc/yum.conf` ou ao seu próprio arquivo `repository.repo` no diretório `/etc/yum.repos.d`. Você pode fazer isso manualmente, mas a maioria dos repositórios yum fornece seu próprio arquivo `repository.repo` no URL do repositório.

Para determinar quais repositórios yum já estão instalados

- Liste os repositórios yum instalados com o seguinte comando:

```
[ec2-user ~]$ yum repolist all
```

A saída resultante lista os repositórios instalados e relata o status de cada um. Os repositórios habilitados exibem o número de pacotes que eles contêm.

Para adicionar um repositório yum a `/etc/yum.repos.d`

1. Encontre a localização do arquivo `.repo`. Isso varia dependendo do repositório que você está adicionando. Neste exemplo, o arquivo `.repo` está em `https://www.example.com/repository.repo`.

2. Adicione um repositório com o comando yum-config-manager.

```
[ec2-user ~]$ sudo yum-config-manager --add-repo https://www.example.com/repository.repo
Loaded plugins: priorities, update-motd, upgrade-helper
adding repo from: https://www.example.com/repository.repo
grabbing file https://www.example.com/repository.repo to /etc/yum.repos.d/repository.repo
repository.repo                                         | 4.0 kB     00:00
repo saved to /etc/yum.repos.d/repository.repo
```

Após instalar um repositório, você deve habilitá-lo como descrito no próximo procedimento.

Para habilitar um repositório yum em **/etc/yum.repos.d**

- Use o comando yum-config-manager com o sinalizador `--enable repository`. O comando a seguir habilita o repositório Extra Packages for Enterprise Linux (EPEL) do projeto Fedora. Por padrão, esse repositório está presente em `/etc/yum.repos.d` em instâncias do Amazon Linux AMI, mas não está habilitado.

```
[ec2-user ~]$ sudo yum-config-manager --enable epel
```

#### Note

Para habilitar o repositório EPEL no Amazon Linux 2, use o seguinte comando:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

Para obter informações sobre como habilitar o repositório EPEL em outras distribuições, como o Red Hat e o CentOS, consulte a documentação do EPEL em <https://fedoraproject.org/wiki/EPEL>.

## Encontrar pacotes de software em uma instância do Amazon Linux

Você pode usar o comando yum search para pesquisar as descrições de pacotes que estão disponíveis nos repositórios configurados. Isso é especialmente útil se você não souber o nome exato do pacote que deseja instalar. Basta acrescentar uma pesquisa de palavra-chave ao comando. Para pesquisar várias palavras, coloque a consulta da pesquisa entre aspas.

#### Important

Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

```
[ec2-user ~]$ sudo yum search "find"
```

Veja a seguir um exemplo de saída para o Amazon Linux 2.

```
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
=====
N/S matched: find =====
findutils.x86_64 : The GNU versions of find utilities (find and xargs)
gedit-plugin-findinfiles.x86_64 : gedit findinfiles plugin
```

```
ocaml-findlib-devel.x86_64 : Development files for ocaml-findlib
perl-File-Find-Rule.noarch : Perl module implementing an alternative interface to
    File::Find
robotfindskitten.x86_64 : A game/zen simulation. You are robot. Your job is to find kitten.
mlocate.x86_64 : An utility for finding files by name
ocaml-findlib.x86_64 : Objective CAML package manager and build helper
perl-Devel-Cycle.noarch : Find memory cycles in objects
perl-Devel-EnforceEncapsulation.noarch : Find access violations to blessed objects
perl-File-Find-Rule-Perl.noarch : Common rules for searching for Perl things
perl-File-HomeDir.noarch : Find your home and other directories on any platform
perl-IPC-Cmd.noarch : Finding and running system commands made easy
perl-Perl-MinimumVersion.noarch : Find a minimum required version of perl for Perl code
texlive-xesearch.noarch : A string finder for XeTeX
valgrind.x86_64 : Tool for finding memory management bugs in programs
valgrind.i686 : Tool for finding memory management bugs in programs
```

Veja a seguir um exemplo de saída para o Amazon Linux.

```
Loaded plugins: priorities, security, update-motd, upgrade-helper
=====
N/S Matched: find =====
findutils.x86_64 : The GNU versions of find utilities (find and xargs)
perl-File-Find-Rule.noarch : Perl module implementing an alternative interface to
    File::Find
perl-Module-Find.noarch : Find and use installed modules in a (sub)category
libpuzzle.i686 : Library to quickly find visually similar images (gif, png, jpg)
libpuzzle.x86_64 : Library to quickly find visually similar images (gif, png, jpg)
mlocate.x86_64 : An utility for finding files by name
```

Consultas de pesquisa de várias palavras entre aspas apenas retornam resultados que correspondem à consulta exata. Se você não vir o pacote esperado, simplifique a pesquisa usando uma palavra-chave e verifique os resultados. Você também pode tentar usar sinônimos da palavras-chave para ampliar a pesquisa.

Para obter mais informações sobre pacotes para o Amazon Linux 2 e o Amazon Linux, consulte o seguinte:

- [Repositório de pacotes \(p. 175\)](#)
- [Biblioteca de extras \(Amazon Linux 2\) \(p. 178\)](#)

## Instalar pacotes de software em uma instância do Amazon Linux

O gerenciador de pacotes yum é uma ótima ferramenta para instalar software, pois ele pode pesquisar todos os repositórios habilitados para diferentes pacotes de software e, além disso, lidar com qualquer dependência no processo de instalação de software.

### Important

Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

Para instalar um pacote a partir de um repositório

Use o comando `yum install package`, substituindo `package` pelo nome do software a ser instalado. Por exemplo, para instalar o navegador da Web baseado em texto links, insira o seguinte comando.

```
[ec2-user ~]$ sudo yum install links
```

Para instalar arquivos de pacotes RPM que você obteve por download

Você também pode usar yum install para instalar arquivos de pacotes de RPM que você obteve por download da Internet. Para fazer isso, adicione o nome do caminho de um arquivo RPM ao comando de instalação em vez de um nome de pacote de repositório.

```
[ec2-user ~]$ sudo yum install my-package.rpm
```

Para listar pacotes instalados

Para ver uma lista de pacotes instalados na instância, use o comando a seguir.

```
[ec2-user ~]$ yum list installed
```

## Preparar-se para compilar software em uma instância do Amazon Linux

Há vários softwares de código aberto disponíveis na Internet que não foram pré-compilados e disponibilizados para download de um repositório de pacotes. Você pode acabar descobrindo um pacote de software que precisa compilar por conta própria, do código-fonte. Para que seu sistema possa compilar software, você precisará instalar várias ferramentas de desenvolvimento, como make, gcc e autoconf.

### Important

Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

Como a compilação de software não é uma tarefa necessária para toda instância do Amazon EC2, essas ferramentas não são instaladas por padrão, mas elas estão disponíveis em um grupo de pacotes chamado "Development Tools", que é adicionado facilmente a uma instância com o comando yum groupinstall.

```
[ec2-user ~]$ sudo yum groupinstall "Development Tools"
```

Os pacotes de código-fonte de software frequentemente estão disponíveis para download (em sites como <https://github.com/> e <http://sourceforge.net/>) como um arquivo compactado, chamado tarball. Esses tarballs geralmente têm a extensão de arquivo .tar.gz. Você pode descompactar esses arquivos com o comando tar.

```
[ec2-user ~]$ tar -xzf software.tar.gz
```

Após descompactar e desarquivar o pacote do código-fonte, você deve procurar um arquivo README ou INSTALL no diretório de código-fonte que pode fornecer instruções adicionais para compilar e instalar o código-fonte.

### Como recuperar o código-fonte dos pacotes do Amazon Linux

A Amazon Web Services fornece o código-fonte para pacotes mantidos. Você pode fazer download do código-fonte de todos os pacotes instalados com o comando yumdownloader --source.

- Execute o comando yumdownloader --source **package** para fazer download do código fonte do **pacote**. Por exemplo, para fazer download do código-fonte para o pacote htop, insira o seguinte comando.

```
[ec2-user ~]$ yumdownloader --source htop
```

```
Loaded plugins: priorities, update-motd, upgrade-helper
```

```
| Enabling amzn-updates-source repository
| Enabling amzn-main-source repository
amzn-main-source
| 1.9 kB 00:00:00
amzn-updates-source
| 1.9 kB 00:00:00
(1/2): amzn-updates-source/latest/primary_db
| 52 kB 00:00:00
(2/2): amzn-main-source/latest/primary_db
| 734 kB 00:00:00
htop-1.0.1-2.3.amzn1.src.rpm
```

O local do RPM de origem está no diretório em que você executou o comando.

## Gerenciar contas de usuário na instância do Amazon Linux

Cada tipo de instância do Linux é executada com uma conta de usuário do sistema Linux padrão. O nome de usuário padrão é determinado pela AMI especificada ao executar a instância.

- Para o Amazon Linux 2 ou a AMI do Amazon Linux, o nome do usuário é `ec2-user`.
- Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
- Para uma AMI do Ubuntu, o nome do usuário é `admin`.
- Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
- Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
- Para uma AMI do Bitnami, o nome do usuário é `bitnami`.
- Caso contrário, verifique com o provedor da AMI.

### Note

Os usuários do sistema Linux não devem ser confundidos com os usuários do AWS Identity and Access Management (IAM). Para obter mais informações, consulte [Usuários IAM](#) no Manual do usuário IAM.

### Tópicos

- [Considerations \(p. 602\)](#)
- [Criar uma conta de usuário \(p. 603\)](#)
- [Remover uma conta de usuário \(p. 604\)](#)

## Considerations

O uso da conta de usuário padrão é adequado para várias aplicações. No entanto, escolha adicionar contas de usuário para que eles possam ter seus próprios arquivos e workspaces. Além disso, a criação de contas de usuário para novos usuários é muito mais segura do que conceder a vários usuários (possivelmente inexperientes) acesso à conta de usuário padrão, pois essa conta pode causar muitos danos a um sistema quando usada de modo inadequado. Para obter mais informações, consulte [Dicas para proteger sua instância do EC2](#).

Para permitir aos usuários acesso SSH à sua instância do EC2 usando uma conta de usuário do sistema Linux, você deve compartilhar a chave SSH com o usuário. Uma outra opção é usar o EC2 Instance Connect para fornecer acesso aos usuários sem precisar compartilhar e gerenciar as chaves SSH. Para obter mais informações, consulte [Conectar-se à instância do Linux usando EC2 Instance Connect \(p. 541\)](#).

## Criar uma conta de usuário

Primeiro crie a conta de usuário e, depois, adicione a chave pública SSH que permite que o usuário se conecte e faça login na instância.

Para criar uma conta de usuário

1. [Crie um novo par de chaves \(p. 1210\)](#). É necessário fornecer o arquivo `.pem` para o usuário para o qual você está criando a conta de usuário. Ele deve usar esse arquivo para se conectar à instância.
2. Recupere a chave pública do par de chaves criado na etapa anterior.

```
$ ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
```

O comando retorna a chave pública, como mostrado no exemplo a seguir.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706Vhz2ItxCih
+PnDSUaw+WNQn/mZphTk/a/gu8jEzoWbkM4yxzb/wB96xbiFveSFJuOp/
d6RJhJOIOiBXrlsLnBItntckiJ7FbtJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/
cQk+0FzZqaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkyQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
+z7wB3RbBQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

3. Conecte-se à instância.
4. Use o comando `adduser` para criar a conta de usuário e adicioná-la ao sistema (com uma entrada no arquivo `/etc/passwd`). O comando também cria um grupo e um diretório inicial para a conta. Neste exemplo, a conta de usuário é chamada `newuser`.
  - Amazon Linux e Amazon Linux 2
  - Ubuntu

```
[ec2-user ~]$ sudo adduser newuser
```

Inclua o parâmetro `--disabled-password` para criar a conta de usuário sem senha.

```
[ubuntu ~]$ sudo adduser newuser --disabled-password
```

5. Mude para a nova conta, de modo que o diretório e o arquivo criados tenham a propriedade adequada.

```
[ec2-user ~]$ sudo su - newuser
```

O prompt é alterado de `ec2-user` para `newuser` para indicar que você mudou a sessão de shell para a nova conta.

6. Adicione a chave pública SSH à conta de usuário. Primeiro, crie um diretório no diretório inicial do usuário para o arquivo de chave SSH. Depois disso, crie o arquivo de chave e, por fim, cole a chave pública no arquivo de chave, conforme descrito nas etapas secundárias a seguir.
  - a. Crie um diretório `.ssh` no diretório inicial `newuser` e altere suas permissões de arquivos para 700 (somente o proprietário pode ler, gravar ou abrir o diretório).

```
[newuser ~]$ mkdir .ssh
```

```
[newuser ~]$ chmod 700 .ssh
```

**Important**

Sem essas permissões de arquivos, o usuário não poderá se conectar.

- b. Crie um arquivo chamado `authorized_keys` no diretório `.ssh` e altere suas permissões de arquivos para 600 (somente o proprietário pode ler ou gravar no arquivo).

```
[newuser ~]$ touch .ssh/authorized_keys
```

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

**Important**

Sem essas permissões de arquivos, o usuário não poderá se conectar.

- c. Abra o arquivo `authorized_keys` usando seu editor de texto favorito (como vim ou nano).

```
[newuser ~]$ nano .ssh/authorized_keys
```

Cole a chave pública recuperada na Etapa 2 no arquivo e salve as alterações.

**Important**

Cole a chave pública em uma linha contínua. A chave pública não deve ser dividida em várias linhas.

Agora, o usuário deve poder se conectar à conta `newuser` em sua instância usando a chave privada correspondente à chave pública adicionada ao arquivo `authorized_keys`. Para obter mais informações sobre os diferentes métodos de conexão a uma instância Linux, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).

## Remover uma conta de usuário

Se uma conta de usuário não for mais necessária, você poderá remover essa conta de modo que ela não possa mais ser usada.

Use o comando `userdel` para remover a conta de usuário do sistema. Quando você especifica o parâmetro `-r`, o diretório inicial e o spool de e-mail do usuário são excluídos. Para manter o diretório inicial e o spool de e-mail do usuário, omita o parâmetro `-r`.

```
[ec2-user ~]$ sudo userdel -r olduser
```

## Controle do estado do processo para a instância do EC2

C-states controlam os níveis de desativação que um núcleo pode assumir quando está inativo. Os C-states são numerados começando com C0 (o estado mais superficial em que o núcleo está totalmente ativo e executando instruções) até C6 (o estado de ociosidade mais profundo em que um núcleo está desativado).

Os P-states controlam a performance desejada (na frequência da CPU) de um núcleo. Os P-states são numerados começando com P0 (a configuração de performance mais elevada em que o núcleo pode usar a Intel Turbo Boost Technology para aumentar a frequência, se possível) e vão de P1 (o P-state que solicita a frequência máxima de linha de base) até P15 (a frequência mais baixa possível).

Os tipos de instâncias a seguir oferecem a capacidade de um sistema operacional de controlar C-states e P-states do processador:

- Uso geral: m4.10xlarge | m4.16xlarge | m5.metal | m5d.metal
- Otimizada para computação: c4.8xlarge | c5.metal | c5n.metal
- Otimizadas para memória: r4.8xlarge | r4.16xlarge | r5.metal | r5d.metal | u-6tb1.metal | u-9tb1.metal | u-12tb1.metal | u-18tb1.metal | u-24tb1.metal | x1.16xlarge | x1.32xlarge | x1e.8xlarge | x1e.16xlarge | x1e.32xlarge | z1d.metal
- Otimizadas para armazenamento: d2.8xlarge | i3.8xlarge | i3.16xlarge | i3.metal | i3en.metal | h1.8xlarge | h1.16xlarge
- Computação acelerada: f1.16xlarge | g3.16xlarge | g4dn.metal | p2.16xlarge | p3.16xlarge

Os tipos de instâncias a seguir oferecem a capacidade de um sistema operacional de controlar C-states do processador:

- Uso geral: m5.12xlarge | m5.24xlarge | m5d.12xlarge | m5d.24xlarge | m5n.12xlarge | m5n.24xlarge | m5dn.12xlarge | m5dn.24xlarge
- Otimizada para computação: c5.9xlarge | c5.12xlarge | c5.18xlarge | c5.24xlarge | c5a.24xlarge | c5ad.24xlarge | c5d.9xlarge | c5d.12xlarge | c5d.18xlarge | c5d.24xlarge | c5n.9xlarge | c5n.18xlarge
- Otimizadas para memória: r5.12xlarge | r5.24xlarge | r5d.12xlarge | r5d.24xlarge | r5n.12xlarge | r5n.24xlarge | r5dn.12xlarge | r5dn.24xlarge | z1d.6xlarge | z1d.12xlarge
- Otimizada para armazenamento: d3en.12xlarge | i3en.12xlarge | i3en.24xlarge
- Computação acelerada: inf1.24xlarge | p3dn.24xlarge

AWSOs processadores Graviton da têm modos de economia de energia integrados e operam em uma frequência fixa. Portanto, eles não fornecem a capacidade para o sistema operacional controlar os C-states e P-states.

Talvez você queira alterar as configurações de C-state ou P-state para aumentar a consistência de performance do processador, reduzir a latência ou ajustar sua instância para uma workload específica. As configurações padrão de C-state e P-state proporcionam o performance máximo, que é o ideal para a maioria das workloads. Contudo, se sua aplicação se beneficiaria de latência reduzida ao custo de frequências superiores de single ou dual core, ou de uma performance consistente em frequências menores em oposição às frequências Turbo Boost intermitentes, considere experimentar as configurações de C-state ou P-state que estão disponíveis para essas instâncias.

As seções a seguir descrevem as diferentes configurações de estado do processador e como monitorar os efeitos de sua configuração. Esses procedimentos foram redigidos para o Amazon Linux e se aplicam a ele; eles também podem funcionar para outras distribuições do Linux com a versão de kernel Linux 3.9 ou mais recente. Para obter mais informações sobre outras distribuições do Linux e controle do estado do processador, consulte a documentação específica do seu sistema.

#### Note

Os exemplos nesta página usam o utilitário turbostat (que está disponível no Amazon Linux por padrão) para exibir a frequência do processador e as informações do C-state, e o comando stress (que pode ser instalado executando sudo yum install -y stress) para simular uma workload. Se a saída não exibe informações do C-state, inclua a opção --debug no comando (sudo turbostat --debug stress <options>).

## Tópicos

- [A mais alta performance com a frequência máxima de Turbo Boost \(p. 606\)](#)
- [Alta performance e baixa latência limitando os C-states mais profundos \(p. 607\)](#)
- [Performance basal com menor variabilidade \(p. 608\)](#)

## A mais alta performance com a frequência máxima de Turbo Boost

Essa é a configuração de controle de estado do processador padrão para o Amazon Linux AMI, e é a recomendada para a maioria das workloads. Essa configuração fornece a mais alta performance com menor variabilidade. Permitir que os núcleos inativos assumam os estados mais profundos de desativação fornece o espaço térmico para processos de single ou dual core a fim de atingir o potencial máximo de Turbo Boost.

O exemplo a seguir mostra uma instância c4.8xlarge com dois núcleos que executam o trabalho de forma ativa, atingindo a frequência Turbo Boost do processador.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [30680] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30680] successful run completed in 10s
pk cor CPU %c0 GHz TSC SMI %c1 %c3 %c6 %c7 %pc2 %pc3 %pc6 %pc7
Pkg_W RAM_W PKG_% RAM_%
      5.54 3.44 2.90  0  9.18  0.00  85.28  0.00  0.00  0.00  0.00  0.00
 94.04 32.70 54.18 0.00
 0   0   0   0.12 3.26 2.90  0  3.61  0.00  96.27  0.00  0.00  0.00
 48.12 18.88 26.02 0.00
 0   0   18  0.12 3.26 2.90  0  3.61
 0   1   1   0.12 3.26 2.90  0  4.11  0.00  95.77  0.00
 0   1   19  0.13 3.27 2.90  0  4.11
 0   2   2   0.13 3.28 2.90  0  4.45  0.00  95.42  0.00
 0   2   20  0.11 3.27 2.90  0  4.47
 0   3   3   0.05 3.42 2.90  0  99.91  0.00  0.05  0.00
 0   3   21  97.84 3.45 2.90  0  2.11
...
 1   1   10  0.06 3.33 2.90  0  99.88  0.01  0.06  0.00
 1   1   28  97.61 3.44 2.90  0  2.32
...
10.002556 sec
```

Neste exemplo, os vCPUs 21 e 28 estão sendo executadas na frequência Turbo Boost máxima porque os outros núcleos entraram no estado de desativação C6 para economizar energia e fornecer energia e espaço térmico para os núcleos ativos. Os vCPUs 3 e 10 (cada um compartilhando um núcleo de processador com vCPUs 21 e 28) estão no estado C1, aguardando instruções.

No exemplo a seguir, todos os 18 núcleos estão executando trabalho de forma ativa, portanto, não há espaço para o Turbo Boost máximo, mas todos eles estão em execução na velocidade "all core Turbo Boost" de 3,2 GHz.

```
[ec2-user ~]$ sudo turbostat stress -c 36 -t 10
stress: info: [30685] dispatching hogs: 36 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30685] successful run completed in 10s
pk cor CPU %c0 GHz TSC SMI %c1 %c3 %c6 %c7 %pc2 %pc3 %pc6 %pc7
Pkg_W RAM_W PKG_% RAM_%
      99.27 3.20 2.90  0  0.26  0.00  0.47  0.00  0.00  0.00  0.00  0.00
    228.59 31.33 199.26 0.00
    0   0   0   99.08 3.20 2.90  0  0.27  0.01  0.64  0.00  0.00  0.00
    114.69 18.55 99.32 0.00
    0   0   18  98.74 3.20 2.90  0  0.62
```

0	1	1	99.14	3.20	2.90	0	0.09	0.00	0.76	0.00
0	1	19	98.75	3.20	2.90	0	0.49			
0	2	2	99.07	3.20	2.90	0	0.10	0.02	0.81	0.00
0	2	20	98.73	3.20	2.90	0	0.44			
0	3	3	99.02	3.20	2.90	0	0.24	0.00	0.74	0.00
0	3	21	99.13	3.20	2.90	0	0.13			
0	4	4	99.26	3.20	2.90	0	0.09	0.00	0.65	0.00
0	4	22	98.68	3.20	2.90	0	0.67			
0	5	5	99.19	3.20	2.90	0	0.08	0.00	0.73	0.00
0	5	23	98.58	3.20	2.90	0	0.69			
0	6	6	99.01	3.20	2.90	0	0.11	0.00	0.89	0.00
0	6	24	98.72	3.20	2.90	0	0.39			
...										

## Alta performance e baixa latência limitando os C-states mais profundos

Os C-states controlam os níveis de desativação que um núcleo pode assumir quando está inativo. É possível controlar os C-states para ajustar seu sistema em relação à latência versus performance. Desativar núcleos leva tempo e, embora um núcleo desativado forneça mais espaço para um núcleo funcionar em uma frequência mais alta, leva tempo para que esse núcleo desativado seja reativado e execute o trabalho. Por exemplo, se um núcleo que receber a tarefa de lidar com interrupções de pacotes da internet estiver desativado, poderá ocorrer um atraso em lidar com essa interrupção. Você pode configurar o sistema para não usar C-states mais profundos, o que reduz a latência de reação do processador, mas que, por sua vez, também reduz o espaço disponível para outros núcleos para Turbo Boost.

Um cenário comum para desabilitar estados de desativação mais profundos é uma aplicação de banco de dados Redis, que armazena o banco de dados na memória do sistema para o tempo de resposta de consulta mais rápido possível.

Para limitar estados de desativação mais profundos no Amazon Linux 2

1. Abra o arquivo `/etc/default/grub` com o editor de preferência.

```
[ec2-user ~]$ sudo vim /etc/default/grub
```

2. Edite a linha `GRUB_CMDLINE_LINUX_DEFAULT` e adicione a opção `intel_idle.max_cstate=1` para definir C1 como o C-state mais profundo para núcleos inativos.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
biosdevname=0 nvme_core.io_timeout=4294967295 intel_idle.max_cstate=1
GRUB_TIMEOUT=0
```

3. Salve o arquivo e saia do editor.
4. Execute o comando a seguir para recompilar a configuração de inicialização.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. Reinicie sua instância para habilitar a nova opção de kernel.

```
[ec2-user ~]$ sudo reboot
```

Para limitar estados de desativação mais profundos no Amazon Linux AMI

1. Abra o arquivo `/boot/grub/grub.conf` com o editor de preferência.

```
[ec2-user ~]$ sudo vim /boot/grub/grub.conf
```

2. Edite a linha `kernel` da primeira entrada e adicione a opção `intel_idle.max_cstate=1` para definir C1 como o C-state mais profundo para núcleos inativos.

```
# created by imagebuilder
default=0
timeout=1
hiddenmenu

title Amazon Linux 2014.09 (3.14.26-24.46.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-3.14.26-24.46.amzn1.x86_64 root=LABEL=/ console=ttyS0
    intel_idle.max_cstate=1
initrd /boot/initramfs-3.14.26-24.46.amzn1.x86_64.img
```

3. Salve o arquivo e saia do editor.
4. Reinicie sua instância para habilitar a nova opção de kernel.

```
[ec2-user ~]$ sudo reboot
```

O exemplo a seguir mostra uma instância `c4.8xlarge` com dois núcleos que executam o trabalho de forma ativa na frequência "all core Turbo Boost" do núcleo.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5322] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5322] successful run completed in 10s
pk cor CPU %c0 GHz TSC SMI %c1 %c3 %c6 %c7 %pc2 %pc3 %pc6 %pc7
Pkg_W RAM_W PKG_% RAM_%
      5.56 3.20 2.90   0 94.44  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
131.90 31.11 199.47 0.00
0   0   0   0.03 2.08 2.90   0 99.97  0.00  0.00  0.00  0.00  0.00  0.00
67.23 17.11 99.76 0.00
0   0   18  0.01 1.93 2.90   0 99.99
0   1   1   0.02 1.96 2.90   0 99.98  0.00  0.00  0.00
0   1   19  99.70 3.20 2.90   0 0.30
...
1   1   10  0.02 1.97 2.90   0 99.98  0.00  0.00  0.00
1   1   28  99.67 3.20 2.90   0 0.33
1   2   11  0.04 2.63 2.90   0 99.96  0.00  0.00  0.00
1   2   29  0.02 2.11 2.90   0 99.98
...
```

Neste exemplo, os núcleos para as vCPUs 19 e 28 estão em execução em 3,2 GHz, e outros núcleos estão no C-state C1 aguardando instruções. Embora os núcleos de trabalho não estejam atingindo a frequência máxima de Turbo Boost, os núcleos inativos responderão com muito mais rapidez a novas solicitações do que o fariam se estivessem no C-state C6 mais profundo.

## Performance basal com menor variabilidade

Você pode reduzir a variabilidade da frequência do processador com P-states. Os P-states controlam a performance desejada (na frequência da CPU) de um núcleo. A maioria das workloads funcionam melhor em P0, o que exige Turbo Boost. No entanto, é possível ajustar seu sistema para obter uma performance consistente em vez de uma performance intermitente que pode acontecer quando as frequências Turbo Boost são habilitadas.

As workloads Intel Advanced Vector Extensions (AVX ou AVX2) podem se desempenhar bem em frequências menores, e as instruções de AVX podem usar mais energia. Executar o processador em uma

frequência menor desabilitando o Turbo Boost pode reduzir a quantidade de energia usada e manter a velocidade mais consistente. Para obter mais informações sobre como otimizar suas configurações de instância e workload para AVX, consulte <http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/performance-xeon-e5-v3-advanced-vector-extensions-paper.pdf>.

Esta seção descreve como limitar estados de desativação mais profundos e desabilitar o Turbo Boost (solicitando o P-state P1) para fornecer baixa latência e menor variabilidade da velocidade do processador para esses tipos de fluxos de trabalho.

Para limitar estados de desativação mais profundos e desabilitar o Turbo Boost no Amazon Linux 2

1. Abra o arquivo /etc/default/grub com o editor de preferência.

```
[ec2-user ~]$ sudo vim /etc/default/grub
```

2. Edite a linha GRUB\_CMDLINE\_LINUX\_DEFAULT e adicione a opção intel\_idle.max\_cstate=1 para definir C1 como o C-state mais profundo para núcleos inativos.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0  
biosdevname=0 nvme_core.io_timeout=4294967295 intel_idle.max_cstate=1"  
GRUB_TIMEOUT=0
```

3. Salve o arquivo e saia do editor.
4. Execute o comando a seguir para recompilar a configuração de inicialização.

```
[ec2-user ~]$ grub2-mkconfig -o /boot/grub2/grub.cfg
```

5. Reinicialize sua instância para habilitar a nova opção de kernel.

```
[ec2-user ~]$ sudo reboot
```

6. Quando você precisar da baixa variabilidade da velocidade do processador que o P-state P1 fornece, execute o seguinte comando para desabilitar o Turbo Boost.

```
[ec2-user ~]$ sudo sh -c "echo 1 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

7. Quando sua workload for concluída, você poderá reabilitar o Turbo Boost com o seguinte comando.

```
[ec2-user ~]$ sudo sh -c "echo 0 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

Para limitar estados de desativação mais profundos e desabilitar o Turbo Boost no Amazon Linux AMI

1. Abra o arquivo /boot/grub/grub.conf com o editor de preferência.

```
[ec2-user ~]$ sudo vim /boot/grub/grub.conf
```

2. Edite a linha kernel da primeira entrada e adicione a opção intel\_idle.max\_cstate=1 para definir C1 como o C-state mais profundo para núcleos inativos.

```
# created by imagebuilder  
default=0  
timeout=1  
hiddenmenu
```

```
title Amazon Linux 2014.09 (3.14.26-24.46.amzn1.x86_64)
root (hd0,0)
kernel /boot/vmlinuz-3.14.26-24.46.amzn1.x86_64 root=LABEL=/ console=ttyS0
intel_idle.max_cstate=1
initrd /boot/initramfs-3.14.26-24.46.amzn1.x86_64.img
```

3. Salve o arquivo e saia do editor.
4. Reinicialize sua instância para habilitar a nova opção de kernel.

```
[ec2-user ~]$ sudo reboot
```

5. Quando você precisar da baixa variabilidade da velocidade do processador que o P-state P1 fornece, execute o seguinte comando para desabilitar o Turbo Boost.

```
[ec2-user ~]$ sudo sh -c "echo 1 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

6. Quando sua workload for concluída, você poderá reabilitar o Turbo Boost com o seguinte comando.

```
[ec2-user ~]$ sudo sh -c "echo 0 > /sys/devices/system/cpu/intel_pstate/no_turbo"
```

O exemplo a seguir mostra uma instância c4.8xlarge com duas vCPUs que executam o trabalho de forma ativa na frequência de núcleo de linha de base, sem Turbo Boost.

```
[ec2-user ~]$ sudo turbostat stress -c 2 -t 10
stress: info: [5389] dispatching hogs: 2 cpu, 0 io, 0 vm, 0 hdd
stress: info: [5389] successful run completed in 10s
pk cor CPU %c0 GHz TSC SMI %c1 %c3 %c6 %c7 %pc2 %pc3 %pc6 %pc7
Pkg_W RAM_W PKG_% RAM%
      5.59 2.90 2.90   0 94.41  0.00  0.00  0.00  0.00  0.00  0.00  0.00
128.48 33.54 200.00 0.00
  0   0   0   0.04 2.90 2.90   0 99.96  0.00  0.00  0.00  0.00  0.00
  65.33 19.02 100.00 0.00
  0   0   18  0.04 2.90 2.90   0 99.96
  0   1   1   0.05 2.90 2.90   0 99.95  0.00  0.00
  0   1   19  0.04 2.90 2.90   0 99.96
  0   2   2   0.04 2.90 2.90   0 99.96  0.00  0.00
  0   2   20  0.04 2.90 2.90   0 99.96
  0   3   3   0.05 2.90 2.90   0 99.95  0.00  0.00
  0   3   21  99.95 2.90 2.90   0 0.05
...
  1   1   28  99.92 2.90 2.90   0 0.08
  1   2   11  0.06 2.90 2.90   0 99.94  0.00  0.00
  1   2   29  0.05 2.90 2.90   0 99.95
```

Os núcleos para vCPUs 21 e 28 estão execução o trabalho de forma ativa na velocidade de processador de linha de base de 2,9 GHz, e todos os núcleos inativos também estão executando na velocidade de linha de base no C-state C1, prontos para aceitar instruções.

## Definir o horário da sua instância do Linux

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 aconteceram. 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 de sua instância não forem definidos 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 da AWS 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. O endereço IPv6 só é acessível no [Instâncias criadas no Sistema Nitro \(p. 210\)](#). 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 da Amazon Linux 2 e da Amazon Linux são sincronizadas com o Amazon Time Sync Service por padrão.

Use os seguintes procedimentos para configurar o Amazon Time Sync Service na sua instância usando o cliente `chrony`. 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 acessar a Internet para que as fontes de hora de NTP externas funcionem.

Para instâncias do Windows, consulte [Definir o horário para uma instância do Windows](#).

#### Tópicos

- [Configurar o tempo para instâncias do EC2 com endereços IPv4 \(p. 611\)](#)
- [Configurar o tempo para instâncias do EC2 com endereços IPv6 \(p. 614\)](#)
- [Alterar o fuso horário no Amazon Linux \(p. 615\)](#)

## Configurar o tempo para instâncias do EC2 com endereços IPv4

Esta seção descreve como definir o tempo para instâncias do EC2 com endereços IPv4 dependendo do tipo de distribuição Linux.

#### Tópicos

- [Configurar o Amazon Time Sync Service no Amazon Linux AMI \(p. 611\)](#)
- [Configurar o Amazon Time Sync Service no Ubuntu \(p. 613\)](#)
- [Configurar o Amazon Time Sync Service no SUSE Linux \(p. 614\)](#)

## Configurar o Amazon Time Sync Service no Amazon Linux AMI

#### Note

Em Amazon Linux 2, o `chrony` já está instalado e configurado para usar o endereço IP do Amazon Time Sync Service.

No Amazon Linux AMI, é necessário editar o arquivo de configuração `chrony` para adicionar uma entrada de servidor para o Amazon Time Sync Service.

Para configurar sua instância do e usar o Amazon Time Sync Service

1. Conecte-se à sua instância e desinstale o serviço NTP.

```
[ec2-user ~]$ sudo yum erase 'ntp*'
```

2. Instale o pacote `chrony`.

```
[ec2-user ~]$ sudo yum install chrony
```

3. Abra o arquivo `/etc/chrony.conf` usando um editor de texto (como vim ou nano). Verifique se o arquivo inclui a seguinte linha:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

Se a linha estiver presente, significa que o Amazon Time Sync Service já está configurado. Nesse caso, siga para a próxima etapa. Caso contrário, adicione a linha depois de todas as outras instruções `server` ou `pool` já presentes no arquivo e salve as alterações.

4. Reinicie o daemon `chrony` (`chronyd`).

```
[ec2-user ~]$ sudo service chronyd restart
```

```
Starting chronyd:
```

```
[ OK ]
```

#### Note

No RHEL e no CentOS (até a versão 6), o nome do serviço é `chrony` em vez de `chronyd`.

5. Use o comando `chkconfig` para configurar o `chrony` para ser iniciado em cada inicialização do sistema.

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

6. Verifique se `chrony` está usando o endereço IP 169.254.169.123 para sincronizar a hora.

```
[ec2-user ~]$ chronyc sources -v
```

```
210 Number of sources = 7
```

```
.-- Source mode '^' = server, '=' = peer, '#' = local clock.  
/ .- Source state '*' = current synced, '+' = combined, '-' = not combined,  
| / '?' = unreachable, 'x' = time may be in error, '-' = time too variable.  
|| | .- xxxx [ yyyy ] +/- zzzz  
|| | | xxxx = adjusted offset,  
|| | | yyyy = measured offset,  
|| | | | zzzz = estimated error.  
|| | | | \\\  
MS Name/IP address          Stratum Poll Reach LastRx Last sample  
=====  
^* 169.254.169.123          3   6    17    43   -30us[ -226us] +/-  287us  
^- ec2-12-34-231-12.eu-west> 2   6    17    43   -388us[ -388us] +/-   11ms  
^- tshirt.heanet.ie          1   6    17    44   +178us[ +25us] +/- 1959us  
^? tbag.heanet.ie           0   6     0     -      +0ns[ +0ns] +/-   0ns  
^? bray.walcz.net            0   6     0     -      +0ns[ +0ns] +/-   0ns  
^? 2a05:d018:c43:e312:ce77:> 0   6     0     -      +0ns[ +0ns] +/-   0ns  
^? 2a05:d018:dab:2701:b70:b> 0   6     0     -      +0ns[ +0ns] +/-   0ns
```

Na saída retornada, `^*` indica a fonte de hora preferida.

7. Verifique as métricas de sincronização da hora informadas pelo `chrony`.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID      : A9FEA97B (169.254.169.123)  
Stratum          : 4  
Ref time (UTC)   : Wed Nov 22 13:18:34 2017  
System time      : 0.000000626 seconds slow of NTP time
```

```
Last offset      : +0.002852759 seconds
RMS offset      : 0.002852759 seconds
Frequency       : 1.187 ppm fast
Residual freq   : +0.020 ppm
Skew             : 24.388 ppm
Root delay       : 0.000504752 seconds
Root dispersion  : 0.001112565 seconds
Update interval  : 64.4 seconds
Leap status      : Normal
```

## Configurar o Amazon Time Sync Service no Ubuntu

É necessário editar o arquivo de configuração `chrony` para adicionar uma entrada de servidor para o Amazon Time Sync Service.

Para configurar sua instância do e usar o Amazon Time Sync Service

1. Conecte-se à sua instância e use `apt` para instalar o pacote `chrony`.

```
ubuntu:~$ sudo apt install chrony
```

### Note

Se necessário, atualize sua instância primeiro executando `sudo apt update`.

2. Abra o arquivo `/etc/chrony/chrony.conf` usando um editor de texto (como vim ou nano). Adicione a seguinte linha antes de todas as outras instruções `server` ou `pool` já presentes no arquivo, e salve as alterações:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Reinicie o serviço `chrony`.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Verifique se `chrony` está usando o endereço IP 169.254.169.123 para sincronizar a hora.

```
ubuntu:~$ chronyc sources -v
```

```
210 Number of sources = 7

      .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
      / .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
      | /  '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
      ||                               .- xxxx [ yyyy ] +/-_
zzzz
      ||     Reachability register (octal) -.          |  xxxx = adjusted
offset,
      ||     Log2(Polling interval) --.           |  |  yyyy = measured
offset,
      ||                           \  |  |  zzzz = estimated
error.
      ||                           |  |  |  \
```

	MS Name/IP address	Stratum	Poll	Reach	LastRx	Last sample	
<hr/>							
320us	^* 169.254.169.123	3	6	17	12	+15us[ +57us]	+/-
1779us	^- tbag.heanet.ie	1	6	17	13	-3488us[-3446us]	+/-
7710us	^- ec2-12-34-231-12.eu-west-	2	6	17	13	+893us[ +935us]	+/-
0ns	^? 2a05:d018:c43:e312:ce77:6	0	6	0	10y	+0ns[ +0ns]	+/-
0ns	^? 2a05:d018:d34:9000:d8c6:5	0	6	0	10y	+0ns[ +0ns]	+/-
0ns	^? tshirt.heanet.ie	0	6	0	10y	+0ns[ +0ns]	+/-
0ns	^? bray.walcz.net	0	6	0	10y	+0ns[ +0ns]	+/-

Na saída retornada, ^\* indica a fonte de hora preferida.

- Verifique as métricas de sincronização da hora informadas pelo chrony.

```
ubuntu:~$ chronyc tracking
```

```
Reference ID      : 169.254.169.123 (169.254.169.123)
Stratum          : 4
Ref time (UTC)   : Wed Nov 29 07:41:57 2017
System time      : 0.000000011 seconds slow of NTP time
Last offset      : +0.000041659 seconds
RMS offset       : 0.000041659 seconds
Frequency        : 10.141 ppm slow
Residual freq    : +7.557 ppm
Skew              : 2.329 ppm
Root delay       : 0.000544 seconds
Root dispersion  : 0.000631 seconds
Update interval  : 2.0 seconds
Leap status       : Normal
```

## Configurar o Amazon Time Sync Service no SUSE Linux

Instale o chrony encontrado em <https://software.opensuse.org/package/chrony>.

Abra o arquivo /etc/chrony.conf usando um editor de texto (como vim ou nano). Verifique se o arquivo contém a seguinte linha:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

Se essa linha não estiver presente, adicione-a. Comente qualquer outro servidor ou linhas de consulta. Abra o yaST e ative o serviço chrony.

## Configurar o tempo para instâncias do EC2 com endereços IPv6

Esta seção explica como o processo descrito em [Configurar o tempo para instâncias do EC2 com endereços IPv4 \(p. 611\)](#) difere se você estiver configurando o Amazon Time Sync Service para instâncias do EC2 que usam um endereço IPv6. Ela não explica todo o processo de configuração do Amazon Time Sync Service. O endereço IPv6 só é acessível no [Instâncias criadas no Sistema Nitro \(p. 210\)](#).

### Note

Não recomendamos usar o endereço IPv4 e as entradas de endereço IPv6 em conjunto em seu arquivo chrony.conf. Os pacotes IPv4 e IPv6 NTP vêm do mesmo servidor local para a sua instância. Você provavelmente obterá resultados mistos com alguns pacotes provenientes do endpoint IPv4 e alguns do endpoint IPv6 se estiver usando os dois ao mesmo tempo.

Dependendo da distribuição Linux que você estiver usando, ao chegar à etapa para editar o arquivo chrony.conf, você estará usando o endpoint IPv6 do Amazon Time Sync Service (`fd00:ec2::123`) em vez do endpoint IPv4 (`169.254.169.123`):

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Salve o arquivo e verifique se chrony está usando o endereço IPv6 `fd00:ec2::123` para sincronizar a hora:

```
[ec2-user ~]$ chronyc sources -v
```

Na saída, se você vir o endereço IPv6 `fd00:ec2::123`, a configuração estará concluída.

## Alterar o fuso horário no Amazon Linux

Por padrão, as instâncias do Amazon Linux seguem o fuso horário UTC (Tempo Universal Coordenado). Você pode alterar o horário em uma instância para a hora local ou para outro fuso horário em sua rede.

### Important

Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

Para alterar o fuso horário de uma instância

- Identifique o fuso horário a ser usado na instância. O diretório `/usr/share/zoneinfo` contém uma hierarquia de arquivos de dados de fuso horário. Navegue a estrutura do diretório no local para localizar um arquivo para seu fuso horário.

```
[ec2-user ~]$ ls /usr/share/zoneinfo
Africa      Chile      GB          Indian       Mideast     posixrules   US
America    CST6CDT   GB-Eire    Iran         MST        PRC         UTC
Antarctica Cuba      GMT         iso3166.tab MST7MDT    PST8PDT    WET
Arctic     EET        GMT0       Israel      Navajo     right      W-SU
...
```

Algumas das entradas nesse local são diretórios (como `America`), e esses diretórios contêm arquivos de fuso horário para cidades específicas. Encontre sua cidade (ou uma cidade em seu fuso horário) para ser usada para a instância.

- Atualize o arquivo `/etc/sysconfig/clock` com o novo fuso horário. Neste exemplo, usamos o arquivo de dados do fuso horário de Los Angeles, `/usr/share/zoneinfo/America/Los_Angeles`.
  - Abra o arquivo `/etc/sysconfig/clock` com seu editor de texto de preferência (como vim ou nano). Você precisa usar sudo com o comando do editor, pois `/etc/sysconfig/clock` é de propriedade de root.

```
[ec2-user ~]$ sudo nano /etc/sysconfig/clock
```

- b. Localize a entrada `ZONE` e altere para o fuso horário (omitindo a seção `/usr/share/zoneinfo` do caminho). Por exemplo, para alterar o fuso horário de Los Angeles, altere a entrada `ZONE` para:

```
ZONE="America/Los_Angeles"
```

#### Note

Não altere a entrada `UTC=true` para outro valor. Essa entrada é para o relógio de hardware e não precisa ser ajustada quando você está configurando um fuso horário diferente em sua instância.

- c. Salve o arquivo e saia do editor de texto.
3. Crie um link simbólico entre `/etc/localtime` e o arquivo de fuso horário para que a instância localize o arquivo de fuso horário quando fizer referência a informações do horário local.

```
[ec2-user ~]$ sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

4. Reinicie o sistema para obter as informações do novo fuso horário em todos os serviços e aplicações.

```
[ec2-user ~]$ sudo reboot
```

5. (Opcional) Confirme se o fuso horário atual foi atualizado para o novo fuso horário usando o comando `date`. O fuso horário atual aparecerá na saída. No exemplo a seguir, o fuso horário atual é PDT, que corresponde ao fuso horário de Los Angeles.

```
[ec2-user ~]$ date
Sun Aug 16 05:45:16 PDT 2020
```

## 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 \(p. 617\)](#)
- [Núcleos de CPU e threads por núcleo de CPU por tipo de instância \(p. 617\)](#)
- [Especificar opções de CPU para a instância \(p. 635\)](#)
- [Visualizar as opções de CPU para a instância \(p. 636\)](#)

## 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 \(p. 635\)](#).
- 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 \(p. 617\)](#).
- Para desabilitar o multithreading, especifique um thread por núcleo.
- Quando você [altera o tipo de instância \(p. 327\)](#) 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 \(p. 617\)](#)
- [Instâncias otimizadas para computação \(p. 619\)](#)
- [Instâncias de uso geral \(p. 622\)](#)
- [Instâncias otimizadas para memória \(p. 628\)](#)
- [Instâncias otimizadas para armazenamento \(p. 633\)](#)

### 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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
inf1.24xlarge	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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
p2.xlarge	4	2	2	1, 2	1, 2
p2.8xlarge	32	16	2	1 a 16	1, 2
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
p4d.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

## 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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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
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
c6g.medium	1	1	1	1	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1 a 4	1
c6g.2xlarge	8	8	1	1 a 8	1
c6g.4xlarge	16	16	1	1 a 16	1
c6g.8xlarge	32	32	1	1 a 32	1
c6g.12xlarge	48	48	1	1 a 48	1
c6g.16xlarge	64	64	1	1 a 64	1
c6gd.medium	1	1	1	1	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1 a 4	1
c6gd.2xlarge	8	8	1	1 a 8	1
c6gd.4xlarge	16	16	1	1 a 16	1
c6gd.8xlarge	32	32	1	1 a 32	1
c6gd.12xlarge	48	48	1	1 a 48	1
c6gd.16xlarge	64	64	1	1 a 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1 a 4	1
c6gn.2xlarge	8	8	1	1 a 8	1
c6gn.4xlarge	16	16	1	1 a 16	1
c6gn.8xlarge	32	32	1	1 a 32	1
c6gn.12xlarge	48	48	1	1 a 48	1
c6gn.16xlarge	64	64	1	1 a 64	1

## 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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
m4.2xlarge	8	4	2	1 a 4	1, 2
m4.4xlarge	16	8	2	1 a 8	1, 2
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6g.medium	1	1	1	1	1
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1 a 4	1
m6g.2xlarge	8	8	1	1 a 8	1
m6g.4xlarge	16	16	1	1 a 16	1
m6g.8xlarge	32	32	1	1 a 32	1
m6g.12xlarge	48	48	1	1 a 48	1
m6g.16xlarge	64	64	1	1 a 64	1
m6gd.medium	1	1	1	1	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1 a 4	1
m6gd.2xlarge	8	8	1	1 a 8	1
m6gd.4xlarge	16	16	1	1 a 16	1
m6gd.8xlarge	32	32	1	1 a 32	1
m6gd.12xlarge	48	48	1	1 a 48	1
m6gd.16xlarge	64	64	1	1 a 64	1
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Otimizar as opções de CPU

---

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
<b>t3a.small</b>	2	1	2	1	1, 2
<b>t3a.medium</b>	2	1	2	1	1, 2
<b>t3a.large</b>	2	1	2	1	1, 2
<b>t3a.xlarge</b>	4	2	2	2	1, 2
<b>t3a.2xlarge</b>	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
<b>r4.large</b>	2	1	2	1	1, 2
<b>r4.xlarge</b>	4	2	2	1, 2	1, 2
<b>r4.2xlarge</b>	8	4	2	1 a 4	1, 2
<b>r4.4xlarge</b>	16	8	2	1 a 8	1, 2
<b>r4.8xlarge</b>	32	16	2	1 a 16	1, 2
<b>r4.16xlarge</b>	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
<b>r5.large</b>	2	1	2	1	1, 2
<b>r5.xlarge</b>	4	2	2	2	1, 2
<b>r5.2xlarge</b>	8	4	2	2, 4	1, 2
<b>r5.4xlarge</b>	16	8	2	2, 4, 6, 8	1, 2
<b>r5.8xlarge</b>	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
<b>r5.12xlarge</b>	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
<b>r5.16xlarge</b>	64	32	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
<b>r5.24xlarge</b>	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36,	1, 2

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
				38, 40, 42, 44, 46, 48	
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
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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
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
r6g.medium	1	1	1	1	1
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1 a 4	1
r6g.2xlarge	8	8	1	1 a 8	1
r6g.4xlarge	16	16	1	1 a 16	1
r6g.8xlarge	32	32	1	1 a 32	1
r6g.12xlarge	48	48	1	1 a 48	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
r6g.16xlarge	64	64	1	1 a 64	1
r6gd.medium	1	1	1	1	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1 a 4	1
r6gd.2xlarge	8	8	1	1 a 8	1
r6gd.4xlarge	16	16	1	1 a 16	1
r6gd.8xlarge	32	32	1	1 a 32	1
r6gd.12xlarge	48	48	1	1 a 48	1
r6gd.16xlarge	64	64	1	1 a 64	1
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
x2gd.medium	1	1	1	1	1
x2gd.large	2	2	1	1, 2	1

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
x2gd.xlarge	4	4	1	1 a 4	1
x2gd.2xlarge	8	8	1	1 a 8	1
x2gd.4xlarge	16	16	1	1 a 16	1
x2gd.8xlarge	32	32	1	1 a 32	1
x2gd.12xlarge	48	48	1	1 a 48	1
x2gd.16xlarge	64	64	1	1 a 64	1
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
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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, 20, 22, 24, 26, 28, 30, 32	1, 2
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

Tipo de instância	vCPUs padrão	Núcleos de CPU padrão	Threads padrão por núcleo	Núcleos de CPU válidos	Threads válidos por núcleo
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 \(p. 628\)](#):

- 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. \(p. 510\)](#).
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. \(p. 510\)](#).

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
```

## Especificar 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. \(p. 510\)](#).
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. \(p. 510\)](#).

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 , como `lscpu`, 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 .

## Alterar o nome do host da instância do Amazon Linux

Quando você executa uma instância, ela recebe um nome de host que é uma forma de endereço IPv4 privado interno. Um nome DNS privado do Amazon EC2 se parece com isto: `ip-12-34-56-78.us-west-2.compute.internal`, em que o nome consiste no domínio interno, o serviço (nesse caso, `compute`), a região e uma forma de endereço IPv4 privado. Parte desse nome do host é exibida no prompt

do shell quando você se conecta à sua instância (por exemplo, ip-12-34-56-78). Sempre que você interrompe e reinicia a instância do Amazon EC2 (a menos que esteja usando um endereço IP elástico), o endereço IPv4 público muda, assim como seu nome DNS público, o nome do host do sistema e o prompt do shell.

#### Important

Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

## Alterar o nome do host do sistema

Se você tiver um nome DNS público registrado para o endereço IP de sua instância (como `webserver.mydomain.com`), poderá configurar o nome do host do sistema para que a instância se identifique como parte do domínio. Assim, o prompt do shell também é alterado, de modo que ele exibe a primeira parte desse nome em vez do nome do host fornecido pela AWS (por exemplo, `ip-12-34-56-78`). Se você não tiver um nome DNS público registrado, ainda assim poderá alterar o nome do host, mas o processo é um pouco diferente.

Para que a atualização do nome do host seja mantida, você deve verificar se a `preserve_hostname` configuração do cloud-init está definida como `true`. Você pode executar o seguinte comando para editar ou adicionar essa configuração:

```
sudo vi /etc/cloud/cloud.cfg
```

Se a configuração `preserve_hostname` não estiver listada, adicione a seguinte linha de texto ao final do arquivo:

```
preserve_hostname: true
```

Para alterar o nome do host do sistema para um nome DNS público

Siga este procedimento se você já tiver um nome DNS público registrado.

1. • No Amazon Linux 2: use o comando `hostnamectl` para definir o nome do host para refletir o nome de domínio totalmente qualificado (como `webserver.mydomain.com`).

```
[ec2-user ~]$ sudo hostnamectl set-hostname webserver.mydomain.com
```

- Para Amazon Linux AMI: em sua instância, abra o arquivo de configuração `/etc/sysconfig/network` em seu editor de preferência e altere a entrada `HOSTNAME` para refletir o nome de domínio totalmente qualificado (como `webserver.mydomain.com`).

```
HOSTNAME=webserver.mydomain.com
```

2. Reinicialize a instância para obter o novo nome do host.

```
[ec2-user ~]$ sudo reboot
```

Como alternativa, é possível reiniciar usando o console do Amazon EC2 (na página Instances (Instâncias), selecione a instância e escolha Instance state (Estado da instância) e Reboot instance (Reiniciar instância)).

3. Conecte-se à sua instância e verifique se o nome do host foi atualizado. O prompt deverá mostrar o novo nome do host (até o primeiro ".") e o comando `hostname` deve mostrar o nome de domínio totalmente qualificado.

```
[ec2-user@webserver ~]$ hostname
```

webserver.mydomain.com

Para alterar o nome do host do sistema sem um nome DNS público

1. • No Amazon Linux 2: use o comando hostnamectl para definir o nome do host para refletir o nome do host do sistema desejado (como **webserver**).

```
[ec2-user ~]$ sudo hostnamectl set-hostname webserver.localdomain
```

- No Amazon Linux AMI: em sua instância, abra o arquivo de configuração /etc/sysconfig/network em seu editor de texto de preferência e altere a entrada HOSTNAME para refletir o nome do host do sistema desejado (como Webserver **webserver**).

```
HOSTNAME=webserver.localdomain
```

2. Abra o arquivo /etc/hosts em seu editor de texto de preferência e altere a entrada começando com **127.0.0.1** para corresponder ao exemplo abaixo, substituindo seu próprio nome do host.

```
127.0.0.1 webserver.localdomain webserver localhost4 localhost4.localdomain4
```

3. Reinicialize a instância para obter o novo nome do host.

```
[ec2-user ~]$ sudo reboot
```

Como alternativa, é possível reiniciar usando o console do Amazon EC2 (na página Instances (Instâncias), selecione a instância e escolha Instance state (Estado da instância) e Reboot instance (Reiniciar instância)).

4. Conecte-se à sua instância e verifique se o nome do host foi atualizado. O prompt deverá mostrar o novo nome do host (até o primeiro ".") e o comando hostname deve mostrar o nome de domínio totalmente qualificado.

```
[ec2-user@webserver ~]$ hostname  
webserver.localdomain
```

## Alterar o prompt do shell sem afetar o nome do host

Se você não quiser modificar o nome do host para sua instância, mas quiser que um nome de sistema mais útil (como **webserver**) seja exibido no lugar do nome privado fornecido pela AWS (por exemplo, ip-12-34-56-78), você poderá editar os arquivos de configuração do prompt do shell para exibir o apelido do sistema em vez do nome do host.

Para alterar o prompt do shell para um apelido de host

1. Crie um arquivo em /etc/profile.d que defina a variável do ambiente chamada NICKNAME para o valor que você deseja no prompt do shell. Por exemplo, para definir o apelido do sistema como **webserver**, execute o seguinte comando.

```
[ec2-user ~]$ sudo sh -c 'echo "export NICKNAME=webserver" > /etc/profile.d/prompt.sh'
```

2. Abra o arquivo /etc/bashrc (Red Hat) ou /etc/bash.bashrc (Debian/Ubuntu) no seu editor de texto favorito (como vim ou nano). Você precisa usar sudo com o comando do editor, pois /etc/bashrc e /etc/bash.bashrc são de propriedade de root.

3. Edite o arquivo e altere a variável do prompt do shell (`PS1`) para exibir seu apelido em vez do nome do host. Encontre a seguinte linha que define o prompt do shell em `/etc/bashrc` ou `/etc/bash.bashrc` (várias linhas adjacentes são mostradas abaixo para fornecer o contexto; procure a linha que começa com [ `"$PS1"`]):

```
# Turn on checkwinsize
shopt -s checkwinsize
[ "$PS1" = "\s-\v\\\$ " ] && PS1="[\u@\h \w]\\\$ "
# You might want to have e.g. tty in prompt (e.g. more virtual machines)
# and console windows
```

Altere o `\h` (o símbolo para hostname) nessa linha para o valor da variável `NICKNAME`.

```
# Turn on checkwinsize
shopt -s checkwinsize
[ "$PS1" = "\s-\v\\\$ " ] && PS1="[\u@$NICKNAME \w]\\\$ "
# You might want to have e.g. tty in prompt (e.g. more virtual machines)
# and console windows
```

4. (Opcional) Para configurar o título nas janelas do shell com um novo apelido, conclua as seguintes etapas.

- a. Crie um arquivo chamado `/etc/sysconfig/bash-prompt-xterm`.

```
[ec2-user ~]$ sudo touch /etc/sysconfig/bash-prompt-xterm
```

- b. Torne o arquivo executável usando o comando a seguir.

```
[ec2-user ~]$ sudo chmod +x /etc/sysconfig/bash-prompt-xterm
```

- c. Abra o arquivo `/etc/sysconfig/bash-prompt-xterm` no seu editor de texto de preferência (como vim ou nano). Você precisará usar sudo com o comando do editor, pois `/etc/sysconfig/bash-prompt-xterm` é de propriedade de `root`.
- d. Adicione a linha a seguir ao arquivo.

```
echo -ne "\033]0;${USER}@${NICKNAME}: ${PWD/#$HOME/~}\007"
```

5. Desconecte-se e conecte-se novamente para obter o novo valor do apelido.

## Alterar o nome do host em outras distribuições do Linux

Os procedimentos desta página são destinados ao uso com o Amazon Linux somente. Para obter mais informações sobre outras distribuições do Linux, consulte a documentação específica e os seguintes artigos:

- [Como atribuo um nome do host estático a uma instância do Amazon EC2 privada executando RHEL 7 ou Centos 7?](#)

## Configurar um DNS dinâmico na instância do Amazon Linux

Quando você executa uma instância do EC2, ela é atribuída a um endereço IP público e a um DNS (Sistema de Nomes de Domínio) público que você pode usar para ter acesso a ela pela Internet. Como há muitos hosts no domínio da Amazon Web Services, esses nomes públicos devem ser longos o suficiente

para que cada nome permaneça exclusivo. Um nome DNS público do Amazon EC2 se parece com isto: `ec2-12-34-56-78.us-west-2.compute.amazonaws.com`, em que o nome consiste no domínio da Amazon Web Services, o serviço (nesse caso, `compute`), a região e uma forma de endereço IP público.

Os serviços DNS dinâmicos fornecem nomes do host DNS personalizados na área de domínio que podem ser fáceis de lembrar e também mais apropriados ao caso de uso do host. Alguns desses serviços também são gratuitos. Você pode usar um provedor DNS dinâmico com o Amazon EC2 e configurar a instância para atualizar o endereço IP associado a um nome DNS público sempre que uma instância for iniciada. Há muitos provedores diferentes à sua escolha, e os detalhes específicos da escolha do provedor e do registro de um nome com ele estão fora do escopo deste guia.

**Important**

Essas informações se aplicam ao Amazon Linux. Para obter informações sobre outras distribuições, consulte a documentação específica.

**Para usar o DNS dinâmico com o Amazon EC2**

1. Cadastre-se com um provedor de serviços DNS dinâmico e registre um nome DNS público com o serviço. Esse procedimento usa o serviço gratuito de [noip.com/free](#) como exemplo.
2. Configure o cliente de atualização de DNS dinâmico. Após registrar um provedor de serviços de DNS dinâmico e um nome DNS público com o serviço, aponte o nome DNS para o endereço IP de sua instância. Muitos provedores (incluindo o [noip.com](#)) permitem que você faça isso manualmente na página da conta em seu site, mas muitos também oferecem suporte a clientes de atualização de software. Se um cliente de atualização estiver sendo executado em sua instância do EC2, o registro DNS dinâmico será atualizado sempre que o endereço IP mudar, como após o desligamento e a reinicialização. Neste exemplo, você instala o cliente noip2, que funciona com o serviço proporcionado pelo [noip.com](#).
  - a. Habilite o repositório de Extra Packages for Enterprise Linux (EPEL) para obter acesso ao cliente noip2.

**Note**

As instâncias do Amazon Linux têm chaves de GPG e informações de repositório para o repositório do EPEL instalado por padrão; porém, as instâncias do Red Hat e do CentOS devem primeiro instalar o pacote `epel-release` antes que você possa habilitar o repositório do EPEL. Para obter mais informações e fazer download da versão mais recente deste pacote, consulte <https://fedoraproject.org/wiki/EPEL>.

- Para Amazon Linux 2:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- Para Amazon Linux AMI:

```
[ec2-user ~]$ sudo yum-config-manager --enable epel
```

- b. Instale o pacote `noip`.

```
[ec2-user ~]$ sudo yum install -y noip
```

- c. Crie o arquivo de configuração. Insira as informações de login e senha quando solicitado e responda às perguntas subsequentes para configurar o cliente.

```
[ec2-user ~]$ sudo noip2 -c
```

- 3. Habilite o serviço `noip`.

- Para Amazon Linux 2:

```
[ec2-user ~]$ sudo systemctl enable noip.service
```

- Para Amazon Linux AMI:

```
[ec2-user ~]$ sudo chkconfig noip on
```

4. Inicie o serviço noip.

- Para Amazon Linux 2:

```
[ec2-user ~]$ sudo systemctl start noip.service
```

- Para Amazon Linux AMI:

```
[ec2-user ~]$ sudo service noip start
```

Esse comando inicia o cliente, que lê o arquivo de configuração (`/etc/no-ip2.conf`) que você criou anteriormente e atualiza o endereço IP para o nome DNS público que você escolher.

5. Verifique se o cliente de atualização definiu o endereço IP correto para o nome DNS dinâmico. Aguarde alguns minutos para que os registros DNS sejam atualizados e tente se conectar à sua instância usando SSH com o nome DNS público que você configurou nesse procedimento.

## Executar comandos na instância do Linux na inicialização

Ao executar uma instância no Amazon EC2, você tem a opção de passar dados de usuário para a instância que podem ser usados para realizar tarefas de configuração comuns automatizadas e até mesmo executar scripts após a inicialização da instância. Você pode passar dois tipos de dados de usuário para o Amazon EC2: scripts de shell e diretivas de cloud-init. Você também pode passar esses dados para o assistente de inicialização como texto simples, como arquivo (isso é útil para executar instâncias usando ferramentas de linha de comando) ou como texto codificado em base64 (para chamadas à API).

Se você estiver interessado em cenários de automação mais complexos, considere usar AWS CloudFormation e AWS OpsWorks. Para obter mais informações, consulte o [AWS CloudFormation User Guide \(Manual do usuário do AWS CloudFormation\)](#) e o [AWS OpsWorks User Guide \(Manual do usuário do AWS OpsWorks\)](#).

Para obter informações sobre a execução de comandos na instância do Windows durante a inicialização, consulte [Executar comandos na instância do Windows na inicialização](#) e [Gerenciar a configuração de instâncias do Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Nos exemplos a seguir, os comandos de [Instalar um servidor Web LAMP no Amazon Linux 2 \(p. 15\)](#) são convertidos em um script de shell e um conjunto de diretivas cloud-init que é executado quando a instância é executada. Em cada exemplo, as seguintes tarefas são executadas pelos dados do usuário:

- Os pacotes de distribuição de software são atualizados.
- O servidor Web necessário, `php`, e os pacotes `mariadb` são instalados.
- O serviço `httpd` é iniciado e ativado por `systemctl`.
- O security group `ec2-user` é adicionado ao grupo apache.

- As permissões de propriedade e de arquivos apropriadas são definidas para o diretório Web e os arquivos contidos nele.
- Uma página Web simples é criada para testar o servidor Web e o mecanismo de PHP.

#### Tópicos

- [Prerequisites \(p. 643\)](#)
- [Dados de usuário e scripts de shell \(p. 643\)](#)
- [Dados do usuário e console \(p. 644\)](#)
- [Diretivas de cloud-init e dados de usuário \(p. 646\)](#)
- [Dados do usuário e AWS CLI \(p. 647\)](#)

## Prerequisites

Os seguintes exemplos supõem que sua instância tem um nome DNS público que é acessível pela Internet. Para obter mais informações, consulte [Etapa 1: executar uma instância \(p. 10\)](#). Você também precisa configurar o security group para permitir conexões SSH (porta 22), HTTP (porta 80) e HTTPS (porta 443). Para obter mais informações sobre esses pré-requisitos, consulte [Configuração para usar o Amazon EC2. \(p. 5\)](#).

Além disso, essas instruções servem ao Amazon Linux 2, e os comandos e as diretivas podem não funcionar para outras distribuições do Linux. Para obter mais informações sobre outras distribuições, como suporte para cloud-init, consulte a documentação específica.

## Dados de usuário e scripts de shell

Se você estiver familiarizado com scripts de shell, esta é a maneira mais fácil e completa de enviar instruções para uma instância na execução. Se você adicionar essas tarefas no momento da inicialização, será necessário mais tempo para iniciar a instância. Você deve reservar alguns minutos extras para que as tarefas sejam concluídas antes de testar se o script de usuário foi concluído com êxito.

#### Important

Por padrão, os scripts de dados do usuário e as diretrizes cloud-init são executados somente durante o ciclo de inicialização quando você inicia uma instância pela primeira vez. Você pode atualizar sua configuração para garantir que seus scripts de dados de usuário e diretrizes cloud-init sejam executados sempre que você reiniciar sua instância. Para obter mais informações, consulte [How can I utilize user data to automatically run a script with every restart of my Amazon EC2 Linux instance? \(Como posso utilizar os dados do usuário para executar automaticamente um script a cada reinicialização da minha instância Linux do Amazon EC2?\)](#) na Central de Conhecimento da AWS.

Os scripts do shell de dados do usuário devem começar com caracteres `#!` e o caminho para o intérprete que você deseja que leia o script (geralmente `/bin/bash`). Para obter uma excelente introdução sobre scripts de shell, consulte [a programação BASH HOW-TO](#) no Projeto de Documentação Linux ([tldp.org](http://tldp.org)).

Os scripts inseridos como dados de usuário são executados como o usuário `root`; portanto, não use o comando `sudo` no script. Lembre-se de que todos os arquivos que você criar serão de propriedade de `root`. Caso precise que usuários não raiz tenham acesso aos arquivos, modifique as permissões em conformidade com o script. Além disso, como o script não é executado interativamente, você não pode incluir os comandos que exigem feedback do usuário (como `yum update` sem o sinalizador `-y`).

Se você usar uma API da AWS, incluindo a CLI da AWS 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 emitir a chamada de API. Para obter mais

informações, consulte [Usar perfis de instâncias](#) no Guia do usuário do IAM. 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](#).

O arquivo de log de saída de cloud-init (`/var/log/cloud-init-output.log`) captura a saída do console para facilitar a depuração de seus scripts após uma execução se a instância não se comportar da maneira desejada.

Quando um script de dados do usuário é processado, ele é copiado para e executado a partir deste diretório `/var/lib/cloud/instances/instance-id/`. O script não é excluído depois de ser executado. Certifique-se de excluir os scripts de dados do usuário de `/var/lib/cloud/instances/instance-id/` antes de criar uma AMI a partir da instância. Caso contrário, o script existirá nesse diretório em qualquer instância iniciada na AMI.

## 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

Siga o procedimento para executar uma instância em [É possível executar uma instância usando o assistente de execução de instância. \(p. 510\)](#), mas, ao acessar the section called “Etapa 3: configurar detalhes da instância” [\(p. 512\)](#) nesse procedimento, copie o script de shell no campo User data (Dados do usuário) e conclua o procedimento de execução.

No script de exemplo abaixo, o script cria e configura nosso servidor Web.

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Reserve tempo suficiente para executar a instância e execute os comandos do script. Depois, verifique se o script concluiu as tarefas previstas.

Em nosso exemplo, em um navegador Web, insira o URL do arquivo de teste PHP criado pelo script. Essa URL é o endereço DNS público da instância seguido por uma barra e o nome do arquivo.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Você deve consultar a página de informações do PHP. Caso não seja possível visualizar a página de informações do PHP, verifique se o security group que você está usando contém uma regra para permitir tráfego HTTP (porta 80). Para obter mais informações, consulte [Adicionar regras a um grupo de segurança \(p. 1233\)](#).

(Opcional) Se o script não tiver realizado as tarefas você esperava ou se você apenas quiser verificar se o script foi concluído sem erros, examine o arquivo de log de saída de cloud-init em `/var/log/cloud-init-output.log` e procure mensagens de erro na saída.

Para informações adicionais de depuração, você pode criar um arquivo multiparte Mime que inclua uma seção de dados de cloud-init com a seguinte diretiva:

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Essa diretiva envia a saída do comando do script para `/var/log/cloud-init-output.log`. Para obter mais informações sobre os formatos de dados de cloud-init e a criação de arquivos multiparte Mime, consulte [Formatos de cloud-init](#).

## Visualizar e atualizar os dados do usuário da instância

Para atualizar os dados do usuário da instância, primeiro é necessário interromper a instância. Se a instância estiver em execução, será possível exibir os dados do usuário, mas não modificá-los.

### 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.

#### New console

##### Para modificar os dados do usuário 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 e 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. Com a instância ainda selecionada, escolha Actions (Ações), Instance settings (Configurações de instância), Edit user data (Editar dados de usuário).
6. Modifique os dados do usuário conforme necessário e escolha Save (Salvar).
7. Reinicie a instância. Os novos dados do usuário ficam visíveis na instância depois que você reiniciá-la. Contudo, os scripts dos dados do usuário não são executados.

#### Old console

##### Para modificar os dados do usuário 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 e escolha Actions, Instance State e Stop. 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. Com a instância ainda selecionada, escolha Actions (Ações), Instance Settings (Configurações de instância), View/Change User Data (Visualizar/alterar dados de usuário).
6. Na caixa de diálogo Visualizar/alterar dados do usuário, atualize os dados do usuário e escolha Salvar.

7. Reinicie a instância. Os novos dados do usuário ficam visíveis na instância depois que você reiniciá-la. Contudo, os scripts dos dados do usuário não são executados.

## Diretivas de cloud-init e dados de usuário

O pacote de cloud-init configura aspectos específicos de uma nova instância do Amazon Linux quando ela é executada. Em particular, ele configura o arquivo `.ssh/authorized_keys` para o usuário `ec2` para que você possa se conectar com sua própria chave privada. Para obter mais informações, consulte [cloud-init \(p. 179\)](#).

As diretivas de cloud-init podem ser passadas a uma instância em execução da mesma forma que um script é passado, embora a sintaxe seja diferente. Para obter mais informações sobre cloud-init, acesse <http://cloudinit.readthedocs.org/en/latest/index.html>.

### Important

Por padrão, os scripts de dados do usuário e as diretrizes cloud-init são executados somente durante o ciclo de inicialização quando você inicia uma instância pela primeira vez. Você pode atualizar sua configuração para garantir que seus scripts de dados de usuário e diretrizes cloud-init sejam executados sempre que você reiniciar sua instância. Para obter mais informações, consulte [How can I utilize user data to automatically run a script with every restart of my Amazon EC2 Linux instance? \(Como posso utilizar os dados do usuário para executar automaticamente um script a cada reinicialização da minha instância Linux do Amazon EC2?\)](#) na Central de Conhecimento da AWS.

Se você adicionar essas tarefas no momento da inicialização, será necessário mais tempo para iniciar uma instância. Você deve reservar alguns minutos extras para que as tarefas sejam concluídas antes de testar se as diretivas de dados de usuário foram concluídas.

Para passar diretivas de cloud-init para uma instância com dados de usuário

1. Siga o procedimento para executar uma instância em [É possível executar uma instância usando o assistente de execução de instância. \(p. 510\)](#), mas, ao acessar [the section called “Etapa 3: configurar detalhes da instância” \(p. 512\)](#) nesse procedimento, insira o texto da diretiva de cloud-init no campo User data (Dados do usuário) e conclua o procedimento de execução.

No exemplo a seguir, as diretivas criam e configuram um servidor Web no Amazon Linux 2. A linha `#cloud-config` na parte superior é necessária para identificar os comandos como diretrizes cloud-init.

```
#cloud-config
repo_update: true
repo_upgrade: all

packages:
- httpd
- mariadb-server

runcmd:
- [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
- systemctl start httpd
- sudo systemctl enable httpd
- [ sh, -c, "usermod -a -G apache ec2-user" ]
- [ sh, -c, "chown -R ec2-user:apache /var/www" ]
- chmod 2775 /var/www
- [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
- [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
- [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
```

- Reserve tempo suficiente para que a instância seja executada e execute as diretivas nos dados de usuário. Depois, verifique se as diretivas concluíram as tarefas previstas.

Em nosso exemplo, em um navegador Web, insira a URL do arquivo de teste PHP criado pelas diretivas. Essa URL é o endereço DNS público da instância seguido por uma barra e o nome do arquivo.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Você deve consultar a página de informações do PHP. Caso não seja possível visualizar a página de informações do PHP, verifique se o security group que você está usando contém uma regra para permitir tráfego HTTP (porta 80). Para obter mais informações, consulte [Adicionar regras a um grupo de segurança \(p. 1233\)](#).

- (Opcional) Se as diretivas não tiverem realizado as tarefas que você esperava ou se você apenas quiser verificar se as diretivas foram concluídas sem erros, examine o arquivo de log de saída em /var/log/cloud-init-output.log e procure mensagens de erro na saída. Para informações adicionais de depuração, você pode adicionar a seguinte linha às diretivas:

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Essa diretiva orientadora envia a saída runcmd para /var/log/cloud-init-output.log.

## Dados do usuário e AWS CLI

Você pode usar AWS CLI 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 \(p. 665\)](#).

No Windows, você pode usar o AWS Tools for Windows PowerShell em vez de usar a AWS CLI. Para obter mais informações, consulte [Dados do usuário e Tools for Windows PowerShell](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Exemplo: especificar dados do usuário na execução

Para especificar dados de usuário ao executar a instância, use o comando [run-instances](#) com o parâmetro --user-data. Com run-instances, a AWS CLI executa codificação de base64 dos dados de usuário para você.

O exemplo a seguir mostra como especificar um script como uma string na linha de comando:

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
--key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
--user-data echo user data
```

O exemplo a seguir mostra como especificar um script usando um arquivo de texto. Certifique-se de usar o prefixo file:// para especificar o arquivo.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
--key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
--user-data file:///my_script.txt
```

A seguir, temos um exemplo de arquivo de texto com um script de shell.

```
#!/bin/bash
yum update -y
```

```
service httpd start  
chkconfig httpd on
```

Exemplo: modificar os dados do usuário de uma instância interrompida

Você pode modificar os dados de usuário de uma instância interrompida usando o comando [modify-instance-attribute](#). Com modify-instance-attribute, a AWS CLI não executa a codificação de base64 dos dados de usuário para você.

- Em um computador Linux, use o comando base64 para codificar os dados de usuário.

```
base64 my_script.txt >my_script_base64.txt
```

- Em um computador Windows, use o comando certutil para codificar os dados de usuário. Para poder usar esse arquivo com a AWS CLI, você deve remover as primeiras (INICIAR CERTIFICADO) e últimas (ENCERRAR CERTIFICADO) linhas.

```
certutil -encode my_script.txt my_script_base64.txt  
notepad my_script_base64.txt
```

Use os parâmetros --attribute e --value para usar o arquivo de texto codificado para especificar os dados de usuário. Certifique-se de usar o prefixo file:// para especificar o arquivo.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData --value file:///my_script_base64.txt
```

Exemplo: limpar os dados do usuário de uma instância interrompida

Para excluir os dados do usuário existentes, use o comando [modify-instance-attribute](#) da seguinte maneira:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Exemplo: visualizar dados do usuário

Para recuperar os dados de usuário de uma instância, use o comando [describe-instance-attribute](#). Com describe-instance-attribute, a AWS CLI não executa a decodificação de base64 dos dados de usuário para você.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData
```

Esta é uma saída de exemplo com dados de usuário com codificação base64.

```
{  
    "UserData": {  
        "Value": "  
IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAtOpzzXJ2aNWnIGh0dHBkIHN0YXJ0CmNoa2NvbmcZpZyBodHRwZCBvbg=="  
    },  
    "InstanceId": "i-1234567890abcdef0"  
}
```

- Em um computador Linux, use a opção --query para obter os dados de usuário codificados e o comando base64 para descodificá-los.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute userData --output text --query "UserData.Value" | base64 --decode
```

- Em um computador Windows, use a opção --query para obter os dados de usuário codificados e o comando certutil para decodificá-los. Observe que a saída codificada está armazenada em um arquivo e a saída decodificada está armazenada em outro arquivo.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
  userData --output text --query "UserData.Value" >my_output.txt
  certutil -decode my_output.txt my_output_decoded.txt
  type my_output_decoded.txt
```

A seguir está um exemplo de saída.

```
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

## 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 \(p. 667\)](#), 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. Para obter uma inicialização detalhada da AMI de exemplo, consulte [Exemplo: valor de índice de execução da AMI \(p. 674\)](#).

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 \(p. 674\)](#).

### 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 \(p. 210\)](#).

## Tópicos

- [Usar IMDSv2 \(p. 650\)](#)
- [Configurar as opções de metadados da instância \(p. 654\)](#)
- [Recuperar metadados da instância \(p. 657\)](#)
- [Trabalhar com dados do usuário da instância \(p. 664\)](#)
- [Recuperar dados dinâmicos \(p. 666\)](#)
- [Categorias de metadados da instância \(p. 667\)](#)
- [Exemplo: valor de índice de execução da AMI \(p. 674\)](#)
- [Documentos de identidade da instância \(p. 677\)](#)

## 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 \(p. 654\)](#).

Para recuperar metadados da instância, consulte [Recuperar metadados da instância \(p. 657\)](#).

### 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 \(p. 210\)](#).

## 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 Linux 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

Você pode executar dois comandos separados ou combiná-los.

#### Comandos separados

Primeiro, gere um token usando o comando a seguir.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600" `
```

Em seguida, use o token para gerar itens de metadados de nível superior usando o comando a seguir.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

#### Comandos combinados

Você pode armazenar o token e combinar os comandos. O exemplo a seguir combina os dois comandos acima e armazena o cabeçalho do token de sessão em uma variável chamada TOKEN.

#### Note

Se houver um erro na criação do token, em vez de um token válido, uma mensagem de erro será armazenada na variável e o comando não funcionará.

```
[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/`
```

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.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v 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 \(p. 663\)](#).

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 \(p. 876\)](#).
- 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 \(p. 876\)](#).

##### [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 \(p. 512\)](#).
  - 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 \(p. 654\)](#).

#### 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

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 \(p. 654\)](#)
- [Modificar as opções de metadados de instância para as instâncias existentes \(p. 656\)](#)

## 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 \(p. 512\)](#).

## 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 de 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 \(p. 512\)](#).

## 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 revertê-la 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
```

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. 667).

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. 210).

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. 650).

Você pode usar uma ferramenta, como o cURL, conforme mostrado no exemplo a seguir.

### 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/
```

### IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

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 \(p. 654\)](#).
- 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 de instância está desativado.

## Exemplos de recuperação de metadados da instância

### Exemplos

- [Obter as versões disponíveis dos metadados da instância \(p. 658\)](#)
- [Obter itens de metadados de nível superior. \(p. 659\)](#)
- [Obter a lista de chaves públicas disponíveis \(p. 661\)](#)
- [Mostrar os formatos nos quais a chave pública 0 está disponível \(p. 662\)](#)
- [Obter a chave pública 0 \(no formato de chave OpenSSH\) \(p. 662\)](#)
- [Obter o ID de sub-rede de uma instância \(p. 663\)](#)

### 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

```
[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/
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

```
[ec2-user ~]$ curl 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 \(p. 667\)](#).

#### 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/
```

```
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
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

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
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

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/
latest/meta-data/ami-id
ami-0abcdef1234567890
```

### IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id  
ami-0abcdef1234567890
```

### IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/  
latest/meta-data/reservation-id  
r-0efghijk987654321
```

### IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id  
r-0efghijk987654321
```

### IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/  
latest/meta-data/local-hostname  
ip-10-251-50-12.ec2.internal
```

### IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname  
ip-10-251-50-12.ec2.internal
```

### IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/  
latest/meta-data/public-hostname  
ec2-203-0-113-25.compute-1.amazonaws.com
```

### IMDSv1

```
[ec2-user ~]$ curl 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

```
[ec2-user ~]$ `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/public-keys/
```

```
0=my-public-key
```

#### IMDSv1

```
[ec2-user ~]$ curl 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

```
[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/public-keys/0/  
openssh-key
```

#### IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/  
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

```
[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/public-keys/0/openssh-key  
ssh-rsa MIICiTCACfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC  
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6  
b24xFDASBgnVBAsTC01BTSDb25zb2x1MRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd  
BgkqhkiG9w0BCQEWEg5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjaONTIxWhcN  
MTIwNDI0MjaONTIxWjCBiDELMAkGA1UEBhMCVVVMxCzAJBgNVBAgTAldBMRAwDgYD  
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgnVBAsTC01BTSDb25z  
b2x1MRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEg5vb25lQGFt  
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIJ  
21uUSfwfEvySwtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T  
rDHudUzG3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzzswY6786m86gpE  
Ibb3OhjZnzcvoAaRHndlQWIMm2nrAgMBAEWDQYJKoZIhvcNAQEFBQADgYEAtCu4  
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb  
FFBjvSfpJl1J00zbhNY5f6GuoEDmFJ10ZxBHjJhyp378OD8uTs7fLvjkx79LjSTb  
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

#### IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key  
ssh-rsa MIICiTCACfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC  
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6  
b24xFDASBgnVBAsTC01BTSDb25zb2x1MRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd  
BgkqhkiG9w0BCQEWEg5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjaONTIxWhcN  
MTIwNDI0MjaONTIxWjCBiDELMAkGA1UEBhMCVVVMxCzAJBgNVBAgTAldBMRAwDgYD  
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWF6b24xFDASBgnVBAsTC01BTSDb25z
```

```
b2x1MRIwEAYDVQQDEw1UZXN0Q21sYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3iyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHd1QWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwax1Aoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJI1J00zbhNYS5f6GuoEDmFJ10ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
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

```
[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/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

IMDSv1

```
[ec2-user ~]$ curl 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 recesso 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 \(p. 210\)](#), 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 iptables para limitar o acesso

O exemplo a seguir usa iptables do Linux e seu módulo owner para impedir que o servidor Web do Apache (com base no ID de usuário da instalação padrão do apache) 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.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner --uid-owner apache --jump REJECT
```

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 accidentalmente 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 ao serviço de metadados da instância por todos os processos, exceto os processos em execução na conta do usuário `trustworthy-user`.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner ! --uid-owner trustworthy-user --jump REJECT
```

#### Note

- Para usar regras de firewall local, você precisa adaptar os comandos do exemplo anterior para se ajustarem a suas necessidades.
- Por padrão, as regras de iptables não são persistentes em todas as reinicializações do sistema. Elas podem ser transformadas em persistentes usando recursos do SO não descritos aqui.
- O módulo `owner` das iptables só corresponderá à associação do grupo se o grupo for o grupo primário de um determinado usuário local. Outros grupos não são correspondidos.

#### Usar PF ou IPFW para limitar o acesso

Se você estiver usando FreeBSD ou OpenBSD, poderá considerar também o uso de PF ou IPFW. Os exemplos a seguir limitam o acesso ao serviço de metadados de instância apenas ao usuário raiz.

#### PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

#### IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

#### Note

A ordem dos comandos PF e IPFW é importante. O padrão de PF e a regra correspondente mais recente, e o padrão de IPFW é a primeira regra correspondente.

## 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 quando você iniciar a instância.

## Especificar os dados do usuário da instância na inicialização

Você pode especificar dados do usuário quando você executar uma instância. Para obter mais informações, consulte [É possível executar uma instância usando o assistente de execução de instância. \(p. 510\)](#) e [Executar comandos na instância do Linux na inicialização \(p. 642\)](#).

## 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 \(p. 645\)](#).

## 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 \(p. 210\)](#).

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

```
[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/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

### IMDSv1

```
[ec2-user ~]$ curl 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

```
[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/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

#### IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Para recuperar dados do usuário em uma instância no seu computador, consulte [Dados do usuário e AWS CLI \(p. 647\)](#).

## Recuperar dados dinâmicos

Para recuperar dados dinâmicos de uma instância em execução, use o seguinte URI.

```
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 \(p. 210\)](#).

Este exemplo mostra como recuperar as categorias de identidade de instância de alto nível.

#### 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/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

#### IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
```

dsa2048

Para obter mais informações sobre dados dinâmicos e os exemplos de como recuperá-los, consulte [Documentos de identidade da instância \(p. 677\)](#).

## 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 \(p. 210\)](#), 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 \(p. 562\)](#) 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
ami-id	O ID da AMI usada para executar a instância.	1,0
ami-launch-index	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
ami-manifest-path	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 <i>unknown</i> .	1,0
ancestor-ami-ids	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 <i>ancestor-amis</i> .	10/10/2007
block-device-mapping/ami	O dispositivo virtual que contém o sistema de arquivos de inicialização/raiz.	15/12/2007
block-device-mapping/ebs N	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	15/12/2007

Dados	Descrição	Versão
	o índice do volume do Amazon EBS (como ebs1 ou ebs2).	
<code>block-device-mapping/eph</code> <code>emeral</code> <code>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 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.	15/12/2007
<code>block-device-mapping/root</code>	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
<code>block-device-mapping/swap</code>	Os dispositivos virtuais associados a swap. Nem sempre presente.	15/12/2007
<code>elastic-gpus/</code> <code>associations/elastic-gpu-id</code>	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
<code>elastic-inference/</code> <code>associations/eia-id</code>	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
<code>events/maintenance/history</code>	Se houver eventos de manutenção da instância concluídos ou cancelados, contém uma string JSON com informações sobre os eventos. Para obter mais informações, consulte <a href="#">Para visualizar o histórico de eventos sobre eventos concluídos ou cancelados (p. 852)</a> .	17/08/2018

Dados	Descrição	Versão
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 <a href="#">Visualizar eventos agendados (p. 849)</a> .	17/08/2018
events/recommendations/rebalance	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 <a href="#">Recomendações de rebalanceamento de instâncias do EC2 (p. 423)</a> .	04-11-2020
hostname	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
iam/info	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 LastUpdated, InstanceProfileArn e InstanceProfileId. Caso contrário, não estará presente.	12/01/2012
iam/security-credentials/ <i>role-name</i>	Se houver uma função do IAM associada à instância, <i>role-name</i> será o nome da função, e <i>role-name</i> conterá as credenciais de segurança temporárias associadas à função (para obter mais informações, consulte <a href="#">Recuperar credenciais de segurança dos metadados da instância (p. 1197)</a> ). Caso contrário, não estará presente.	12/01/2012

Dados	Descrição	Versão
<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
<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   shutdown   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 <a href="#">Opções de compra de instância (p. 338)</a> .	01/10/2019
<code>instance-type</code>	O tipo da instância. Para obter mais informações, consulte <a href="#">Tipos de instância (p. 203)</a> .	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

Dados	Descrição	Versão
mac	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
metrics/vhostmd	Não está mais disponível.	01/05/2011
network/interfaces/macs/mac/device-number	O número de dispositivo exclusivo associado a essa interface. O número do dispositivo corresponde ao nome do dispositivo; por exemplo, um device-number de 2 é para o dispositivo eth2. Essa categoria corresponde aos campos DeviceIndex e device-index que são usados pelos comandos da API do Amazon EC2 e do EC2 para a AWS CLI.	01/01/2011
network/interfaces/macs/mac/interface-id	O ID da interface de rede.	01/01/2011
network/interfaces/macs/mac/ipv4-associations/public-ip	Os endereços IPv4 privados que estão associados a cada endereço IP público e estão atribuídos a essa interface.	01/01/2011
network/interfaces/macs/mac/ipv6s	Os endereços IPv6 associados à interface. Retornados apenas para instâncias executadas em uma VPC.	30/06/2016
network/interfaces/macs/mac/local-hostname	O nome do host local da interface.	01/01/2011
network/interfaces/macs/mac/local-ipv4s	Os endereços IPv4 privados associados à interface.	01/01/2011
network/interfaces/macs/mac/mac	O endereço MAC da instância.	01/01/2011
network/interfaces/macs/mac/network-card-index	O índice da placa de rede. Alguns tipos de instância suportam várias placas de rede.	01-11-2020
network/interfaces/macs/mac/owner-id	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

Dados	Descrição	Versão
<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 <a href="#">Using DNS with Your VPC</a> .	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
<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

Dados	Descrição	Versão
placement/partition-number	O número da partição na qual a instância é executada.	24/08/2020
placement/region	A região da AWS na qual a instância é executada.	24/08/2020
product-codes	AWS Marketplace Os códigos de produtos associados com a instância, se houver.	01/03/2007
public-hostname	O DNS público da instância. Essa categoria só será retornada se o atributo enableDnsHostnames for definido como true. Para obter mais informações, consulte <a href="#">Usar DNS com a VPC</a> , 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 network/interfaces/mac/ <i>mac</i> /security-groups.	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 aws. Se você tem recursos em outras partições, a partição é aws- <i>partitionname</i> . Por exemplo, a partição de recursos na região China (Pequim) é aws-cn.	20/10/2015

Dados	Descrição	Versão
<code>spot/instance-action</code>	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 <a href="#">instance-action (p. 433)</a> .	15/11/2016
<code>spot/termination-time</code>	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 <a href="#">termination-time (p. 433)</a> .	05/11/2014

## Categorias de dados dinâmicos

A tabela a seguir lista as categorias de dados dinâmicos.

Dados	Descrição	Versão
<code>fws/instance-monitoring</code>	O valor que mostra se o cliente habilitou o monitoramento de um minuto detalhado no CloudWatch. Valores válidos: <code>enabled</code>   <code>disabled</code>	04/04/2009
<code>instance-identity/document</code>	O JSON que contém os atributos da instância, como o ID da instância, o endereço IP privado, etc. Consulte <a href="#">Documentos de identidade da instância (p. 677)</a> .	04/04/2009
<code>instance-identity/pkcs7</code>	Usado para verificar a autenticidade e o conteúdo do documentos em relação à assinatura. Consulte <a href="#">Documentos de identidade da instância (p. 677)</a> .	04/04/2009
<code>instance-identity/signature</code>	Os dados que podem ser usados por outras partes para verificar sua origem e autenticidade. Consulte <a href="#">Documentos de identidade da instância (p. 677)</a> .	04/04/2009

## Exemplo: valor de índice de execução da AMI

Este exemplo demonstra como usar dados do usuário e metadados da instância para configurar suas instâncias.

### 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 \(p. 210\)](#).

Alice deseja executar quatro instâncias de sua AMI de banco de dados favorita, em que a primeira atua como a instância original e as três restantes como réplicas. Ao executá-las, ela deseja adicionar dados do usuário sobre a estratégia de replicação para cada réplica. Ela sabe que esses dados estarão disponíveis para todas as quatro instâncias, então, ela precisa estruturar os dados do usuário de forma que permita a cada instância reconhecer quais partes são aplicáveis a ela. Ela pode fazer isso usando o valor de metadados da instância `ami-launch-index`, que será exclusivo para cada instância. Se você iniciar mais de uma instância ao mesmo tempo, o `ami-launch-index` indicará a ordem em que as instâncias foram executadas. O valor da primeira instância iniciada é 0.

Veja a seguir os dados de usuário construídos por Alice.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

Os dados `replicate-every=1min` definem a configuração da primeira réplica, `replicate-every=5min` definem a configuração da segunda réplica e assim por diante. Alice decide fornecer esses dados como uma string ASCII com um símbolo de pipe (|) que limita os dados para as instâncias separadas.

Alice executa quatro instâncias usando o comando `run-instances` e especificando os dados do usuário.

```
aws ec2 run-instances \
--image-id ami-0abcdef1234567890 \
--count 4 \
--instance-type t2.micro \
--user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Depois de executadas, todas as instâncias têm uma cópia dos dados do usuário e os metadados comuns mostrados aqui:

- ID da AMI: ami-0abcdef1234567890
- ID da reserva: r-1234567890abcabc0
- Chaves públicas: nenhuma
- Nome do security group: padrão
- Tipo de instância: t2.micro

No entanto, cada instância tem determinados metadados exclusivos.

### Instância 1

Metadados	Valor
instance-id	i-1234567890abcdef0
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

## Instância 2

Metadados	Valor
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

## Instância 3

Metadados	Valor
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

## Instância 4

Metadados	Valor
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice pode usar o valor `ami-launch-index` para determinar qual parte dos dados do usuário é aplicável a uma instância específica.

1. Ela se conecta a uma das instâncias e recupera o `ami-launch-index` dessa instância para garantir que ela seja uma das réplicas:

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/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/ami-launch-index
```

Para as etapas a seguir, as solicitações do IMDSv2 usam o token armazenado do comando anterior do IMDSv2, supondo-se que o token não tenha expirado.

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index  
2
```

2. Ela salva o ami-launch-index como uma variável.

IMDSv2

```
[ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN" -v  
http://169.254.169.254/latest/meta-data/ami-launch-index`
```

IMDSv1

```
[ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-  
launch-index`
```

3. Ela salva os dados do usuário como uma variável.

IMDSv2

```
[ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN" -v  
http://169.254.169.254/latest/user-data`
```

IMDSv1

```
[ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
```

4. Finalmente, Alice usa o comando cut para extrair a parte dos dados do usuário aplicável à instância.

IMDSv2

```
[ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"  
replicate-every=5min
```

IMDSv1

```
[ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"  
replicate-every=5min
```

## 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 \(p. 210\)](#).

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>marketplaceProductCode</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

```
$ 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/dynamic/
instance-identity/document
```

## IMDSv1

```
$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

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 \(p. 680\)](#)
- [Usar a assinatura codificada em base64 para verificar o documento de identidade da instância \(p. 683\)](#)
- [Usar a assinatura RSA-2048 para verificar o documento de identidade da instância \(p. 687\)](#)

## 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.

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 e adicione-a a um arquivo chamado `pkcs7` junto com o cabeçalho e rodapé necessários. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
$ echo "-----BEGIN PKCS7-----" >> pkcs7 \
&& 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/
dynamic/instance-identity/pkcs7 >> pkcs7 \
&& echo "" >> pkcs7 \
&& echo "-----END PKCS7-----" >> pkcs7
```

IMDSv1

```
$ echo "-----BEGIN PKCS7-----" >> pkcs7 \
&& curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7 >> pkcs7 \
&& echo "" >> pkcs7 \
&& echo "-----END PKCS7-----" >> pkcs7
```

3. Adicione o conteúdo do documento de identidade da instância dos metadados da instância a um arquivo chamado `document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

IMDSv2

```
$ 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/
dynamic/instance-identity/document >> document
```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
>> document
```

4. Adicione o certificado público DSA da AWS a um novo arquivo chamado `certificate`. Use um dos seguintes comandos dependendo da Região da 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.

```
$ echo "-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw
FwYDVQQIEExBXXXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIEExBXXXNoaW5ndG9u
```

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Metadados da instância e dados do usuário

```
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1  
cnZpY2VzIExmQzCCAbcgwgEsBgcqhkjOOAQBMIIBhKBgQCjkvcS2bb1VQ4yt/5e  
ih5O06kK/n1Lz1lr7D8ZwtQ8fOEpp5E2ng+D6UD1Z1gYipr58Kj3nssSNpI6bx3  
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8ftUpt3QbyYXJdmVMegN6P  
hviYt5JH/nY14h3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j  
k+tqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAoXau8Qe+MBcJ1/U  
hhy1KHvpCG19fueQ2s6IL0Ca0/buycU1CiYQk40KNHCchfNiZbdlx1E9rpUp7bnF  
1Ra2v1ntMX3caRVddbtPEWmdxSCYsYFDk4mzrOLBA4GEAAkBgEbmeve5f8LIE/Gf  
MNmP9CM5eovQOGx5ho8Wqd+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx411HW  
MXrs3IgIB6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw  
vSeDCOUMYQR7R9LINYwouHIZiqQYMAkGByqGSM44BAMDlwAwLAIUWXBlk40xtTwSw  
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6Rok0k9K  
-----END CERTIFICATE-----" >> certificate
```

### Hong Kong Region

O certificado público da AWS da região Hong Kong é o seguinte:

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQMDFwxCzAJBgnVBAYTA1VTMRkw  
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExmQzAeFw0xOTAYMDMwMjIxMjFaFw00  
NTAyMDMwMjIxMjFaMFwxCzAJBgnVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u  
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1  
cnZpY2VzIExmQzCCAbcgwgEsBgcqhkjOOAQBMIIBhKBgQDvQ9RzVvf4MAwGbqfx  
b1CvCoVb99570kLGn/04CowHxJ+vTBR7eyla6AoXltsQXB0mrJswToFKKxT4gbuw  
jK7s9QQX4CmTRwcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LwnNfGsX2cwjcRWHYgi  
71vnubNBzLQhdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOOG  
eSNmxpW4QFu4pIlAyk6EnTZKHT87gdXkAkfo5AfOxxhnE2HezzH9Ap2tMV5  
8bwNvoPHvoKCQwfm+OUB1AxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I50  
x9QdImJpOihL410dYvy9xUoOz+DzFAW8+y1WVYpA4GFAAKBqQDbnBAKSxWr9QHY  
6Dt+EFdGz61AZLeDeBKpaP53Z1DT034J0C5YbJTwBTFGqPtOLxnUVdlGiD6GbmC  
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvhWVnLJkFJ  
9pdOu/ibRPH11E2nz6pK7GboQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC  
cLoM4p/jtVF0j26xbgIUUS4pDKyHaG/eaygLttFpFJqzWHc=  
-----END CERTIFICATE-----" >> certificate
```

### Bahrain Region

O certificado público da AWS da região Bahrain é o seguinte:

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQMDFwxCzAJBgnVBAYTA1VTMRkw  
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExmQzAeFw0xOTAYMDUxMzA2MjFaFw00  
NTAyMDUxMzA2MjFaMFwxCzAJBgnVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u  
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1  
cnZpY2VzIExmQzCCAbcgwgEsBgcqhkjOOAQBMIIBhKBgQDcwojQfgWdv1qli0OB  
8n6cLZ38VE7ZmrjZ9QV//Gst6S1h7euhC23YppKXi1zovefSDwFU54z13/oJ++q  
PH1p1WGL8IZ34UgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG  
fz2Kbw/Dd8JfoPS7KaSCmJKxXQ1VAZbIaDFRGA2qcMkW2HWASyND17bAoGBAnTz  
1dhfMq+1215iofY2oj3HI21Kj3LtZrWEg3W+/4rvhL31TmONne1rl9yGujrjQwy5  
Zp9V4A/w9w2010Lx4K6hj34Eefy/aQnZwNdNhv/FQP7AzOfju+Yl6L130OHqrL0z  
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBqQCVS7m77nuNALz8  
wvUqcooxXMPkxF154NxAsAul9KP9KN4svm0O3Zrb7t2F0tXRM8zU3TqMpryq1o5  
mpMpsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr  
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGwm5ED1  
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXhjuQ==  
-----END CERTIFICATE-----" >> certificate
```

## Cape Town Region

O certificado público da AWS da região Cidade do Cabo é o seguinte:

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIC7DCCAqwCCQCnCbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw  
FwYDVQQIExBXYXN0aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIEzM0zAeFw0xOTA2MDQxMjQ4MDVaFw00  
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXN0aW5ndG9u  
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1  
cnZpY2VzIEzM0zAeFw0xOTA2MDQxMjQ4MDVaFw00NTA2MDQxMjQ4MDVaFw00  
pQBSCHWmn2qeoQTMVWqe50fnTd0zGfxDdIjKxUk58/8zjWG5uR4TXRzmZpGpmXB  
bSuFAR6BGqud2LnT/HIWGJAsnX2u0tSyNfCoJigqwhaea5w+CqZ6I7iBDdnB4TtTw  
q06TlnExHFVj8LMky1ZgiaE1CQIVAIhdobse4K0QnbAhCLER2euQzloXAoGAV/21  
WUuMz/79Ga0JvQcz1FNy1sT0p0u9rU4TengLQIt5iccn/7EIfNtvVO5TzKuIKq7J  
gXzr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17Wzv/76adywIsnDKq  
ekfe15jinaX8MsKUdyDK7Y+ifCG4Pvh0M4+W2XwDgYQAAoGAIxOKbVgwLxrn6Pi2  
6hBoihFv16jKxQ10hHzXJL0Vv9QwnqjJJRF0Cy3dB0zicLxiIxelIdYfvqJr+u  
h1N8rGxEZYyJBEUKMGvscODW85jonXz0bNfcP0aaKH01KKVJL+OZi5n2kn9wgdo5  
F3CVnM18BuR8A1Tr2yrrE6TVZ4wCQYHKoZ1zjgEAwMvADAsAhQfa7MCJZ+/TEY5  
AUr0J4wm8Vzj0AIUSYVu2NdRJ/ERPmDfhW5Esjh1CA=-----END CERTIFICATE-----" >> certificate
```

## Milan Region

O certificado público da AWS da região Milão é o seguinte:

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIC7TCCAqwCCQCME1HPdwG37jaJBgcqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw  
FwYDVQQIExBXYXN0aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD  
VQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIEzM0zAeFw0xOTA0MjkyMDM1MjJaFw00  
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXN0aW5ndG9u  
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1  
cnZpY2VzIEzM0zCCAbYwggErBgcqhkjOOAQBMIIHGKBgQDAkoL4YfdMI/MrQ0oL  
NPfeEk94eiCQA5xNONu7+2eVQtEqjFbDADFEh1p3sh9Q9OheLFH8qpSfNDWn/0  
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJmT  
HJSKSSvUgpdDIRvJXuyB0zdB+wIVALQ3OLeVGd1PMNfS1nD/Yyn+32wNaOGAPBQ3  
7XHg5NLOS4326eFRUT+4ornqFjjP6dp3p0BEzpImNmZTtkCNNUKE4Go9hv5T4lh  
R0p0DVwV0CUpMAZVBp9Obp1XPCyEZtuDqVa7ukPOUpQNqOhLLAqkigTyXVOSmt  
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV10EQPYQUG5/M3xf  
6vE7jKTxxjFWEyjKfJK7PZCzOIGrE/swgAC4PYQW+AwcUweS1K/Hx2oZVUKzWo  
wDUbeu65DcRdw2rSwCbBTU34s1tFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBElv  
uaMQmgOYeZ5eof104GtqPl+1hcQwCQYHKoZ1zjgEAwMwADAtAhQdoeWLrkm0K49+  
AeBK+j6m2h9SKQIVAIbnhS2a8cQVABDCQXVXrc0tOm08-----END CERTIFICATE-----" >> certificate
```

## China Regions

O certificado público da AWS para as regiões China (Pequim) e China (Ningxia) é o seguinte.

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsfADBCmQswCQYDVQQGEwJV  
UzEZMBcGA1UECBMqV2FzaGluZ3RvbIBTDGF0ZTEQMA4GA1UEBxMHU2VhdHRSZTEg  
MB4GA1UEChMXQW1hem9uIFd1YIBTZXJ2aWN1cyBMTEMwIBcNMTUwNTEzMDk1OTE1  
WhgPMjE5NDEwMTYwOTU5MTVamFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXN0  
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24g  
V2ViIFNlcnPzY2VzIEzM0zCCAS1wDQYJKoZ1hvcNAQEBBQADggEPADCCAQoCggEB  
AMWk9vypSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTs8tQqtNloaQcqhto/l  
gsw9+QSnEJeYWnmivJWBdn9CyDpN7cpHVmeGgnJL2fvImWyWe2f2Kq/BL917N7C  
P2ZT52/sH9orlck1n2z08xPi7MItgPHQwu30xsGQsAdWucdxjHGtdchulpo1uJ31  
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
```

```
vtBj/SM4/IgQ3xJslFc190TzbQbgxiI88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWf0Ody0+OoECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdzN2+0E
V1BFr3DPWJHWrf1b7z1+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GETqhzUqteY7
zAeoLrVu/7OynRyfQetJVGichaaxLNm3lcr6kcxOowb+WQO84cwrB3keykH4gRX
KHB2rlWSxta+2panSE01JX2q5jhcfP90rDOTZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbOp1peGC19idOUqxPxWsasWxQX0azYsP
9RyWLHKxH1dMuA==

-----END CERTIFICATE-----" >> certificate
```

## GovCloud Regions

O certificado público da AWS para as regiões GovCloud da AWS é o seguinte.

```
$ echo "-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTA1VTMRkw
FYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYD
VQQKExdBbWF6b24gV2ViFNlcnPZVzIExmQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViFN1
cnZpY2VzIExmQzCCAbcwggEsBgcqhkjOOAQBMIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5O06kK/n1Lz1lr7D8ZwtQP8fOEpp5E2ng+D6UD1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nY14h3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tKqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAoXau8Qe+MBcJ1/U
hy1KHVpCG19fueQ2s6IL0Ca0/buycU1C1YQk40KNHCchfNiZbdIx1E9rpUp7bnF
1Ra2v1ntMX3caRVDbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmp9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKm1lqx411HW
MXrs3IgIb6+hUIB+S8dz8/mm00bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCouMYQR7R9LINYwouHIziqYMAkGBByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----" >> certificate
```

5. Use o comando OpenSSL smime para verificar a assinatura. Inclua a opção `-verify` para indicar que a assinatura precisa ser verificada, e a opção `-noverify` para indicar que o certificado não precisa ser verificado.

```
$ openssl smime -verify -in pkcs7 -inform PEM -content document -certfile certificate -
noverify
```

Se a assinatura for válida, a mensagem `Verification successful` será exibida. Se não for possível verificar a assinatura, 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 do certificado público RSA da AWS

1. Conecte-se à instância.
2. Recupere a assinatura codificada em base64 dos metadados da instância, converta-a em binário e adicione-o a um arquivo chamado `signature`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

## IMDSv2

```
$ 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/dynamic/instance-identity/signature | base64 -d >> signature
```

## IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature | base64 -d >> signature
```

3. Recupere o documento de identidade da instância de texto simples dos metadados da instância e adicione-o a um arquivo chamado `document`. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

## IMDSv2

```
$ 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/dynamic/instance-identity/document >> document
```

## IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document >> document
```

4. Adicione o certificado público RSA da AWS a um novo arquivo chamado `certificate`. Use um dos seguintes comandos, de acordo com a Região da 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.

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDIjCCAougAwIBAgIJAKnL4UEDMN/FMA0GCSqGSIb3DQEBCUAMGoxCzAJBgNV
BAYTA1VTMRMwEQYDVQQIEwpXYXNoaw5ndG9uMRAwDgYDVQQHEwdTZWF0dGx1MRgw
FgYDVQKEw9BbWF6b24uY29tIELuYy4xGjAYBgvNBAMTEWVjMi5hbWF6b25hd3Mu
Y29tMB4XDTE0MDYwNTE0MjgwMloXTDTI0MDYwNTE0MjgwMlowajELMAkGA1UEBhMC
VVMxEzARBgNVBAgTCldhc2hpbdM24xEADOBgNVBAcTB1NLYXR0bGUxGDAWBgNV
BAoTD0FTYXpbvi5jb20gSW5jLjEaMBgGA1UEAxMRZWMylmFtYXpvbmF3cy5jb20w
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBA19GN//SRK2knbjySG0ho3yqqM3
e2TDhW0D2e8+XZqck754gFS099Abt2RmXClamb17xsYHZFapbELC4H91ycihvrD
jbST1ZjkLQgggaONE1q43eS68ZeTDccScXQSNivS1zJZS8HJZjgzB1XjZftjtdJL
XeE4hwvoOsD4f3j9AgMBAAGjgc8wgcvwHQYDVROOBByEFCXWzAgVyrbwnFncFFIs
77VBd1E4MIGcBgNVHSMEgZQwZGAFCXWzAgVyrbwnFncFFIs77VBd1E40W6kbDBq
MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2Vh
dHRsZTEYMBGA1UEChMPQW1hem9uLmNvbSBjbmMuMRowGAYDVQoDEXFlYzIuYW1h
em9uYXdzLmNvbYIJAknL4UEDMN/FMAwGA1UdEwQFMANBAf8wDQYJKoZIhvcNAQEF
BQADgYEAFYcz1OgEhQBXIwIdsgCOS8vEtijYF+j9uO6jz7V0mJqO+pR1AbR1vY8T
C1haGgSI/A1uZUKs/Zfnph0oEI0/hu1IIJ/SKBDtN51vmZ/IzbOPIJWirlsllQIO
7zvWbGd9c9+Rm3p04oTvhu99la7kZqevJK0QRD/6NpCKsqP/0=
-----END CERTIFICATE-----" >> certificate
```

### Hong Kong Region

O certificado público da AWS da região Hong Kong é o seguinte:

```
$ echo "-----BEGIN CERTIFICATE-----  
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV  
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBGA1UE  
ChMPQW1hem9uLmNvbSBJbmMuRowGAYDVQODExF1YzIuY1hem9uYXdzLmNvbTAe  
FwOxOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTA1VTMRMw  
EQYDVQOIEwpXYXNoaW5ndG9uMRAwDgYDVQHEwdTZWF0dGx1MRgwFgYDVQOKEw9B  
bWF6b24uY29tIEluYy4xGjAYBgnVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G  
CSqGSib3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JhjTieHAgacaQkiR  
Pity9QPDE3b+NxDh4UdP1xdIw73JcIIG3sG9RhWiXVCCh6KkuCTqJfPUknIKk8vs  
M3RXf1UpBe8Pf+P92pxqPMCz1Fr2NehsS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY  
Rh84dK98VwIDAQABMA0GCSqGSib3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN  
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo  
TpYM5Bq57gJzDRaBOnQBx9bgHiUwx6XZWaTS/6xjRJDT5p3S1E0mPI31P/eJv4o  
Ezk5zb3eIf10/sqt4756  
-----END CERTIFICATE-----" >> certificate
```

### Bahrain Region

O certificado público da AWS da região Bahrain é o seguinte:

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIDPDCCAqWgAwIBAgIJAM1uIV/zqJFMA0GCSqGSib3DQEBCwUAMHIxCzAJBgNV  
BAYTA1VTMRMwEQYDVQOIIDApXYXNoaW5ndG9uMRAwDgYDVQOHDAdTZWF0dGx1MSAw  
HgYDVQOKDBdBbWF6b24gV2ViIFNlcnPzY2VzIExmQzEaMBgGA1UEAwRZWMylMfT  
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjlxNDMyNddamHIX  
CzAJBgNVBAYTA1VTMRMwEQYDVQOIIDApXYXNoaW5ndG9uMRAwDgYDVQOHDAdTZWF0  
dGx1MSAwHgYDVQOKDBdBbWF6b24gV2ViIFNlcnPzY2VzIExmQzEaMBgGA1UEAwR  
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvCNAQEBBQADgY0AMIGJaoGBALVN  
CDTZenIeoX1SEYqq6k1BV0Z1pvy5y3KnoOreCAE589TwS4MX5+8Fd6AmACmugeBP  
Qk7Hm6b2+g/d4tWycyxLaQ1lcq81DB1GmXehRkZRgGeRge1ePwD1TUA0I8P/QBT7S  
gUePm/kANSFU+P7s7u1NNl+vynyioWUUrw7/wIZTAgMBAAGjgdccwgdQwHQYDVR0O  
BBYEFILtMd+T4YgH1cgch+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH  
1cgch+hVsVOV+480FoXakdDByM0swCQYDVQOGEwJVVuzETMBEGA1UECAwKV2FzaGlu  
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFd1YiBTZXJ2  
aWNlcyBMTEMxGjAYBgnVBAMMEWjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw  
DAYDVR0TBauAwEB/zANBgkqhkiG9w0BAQsFAAOBgQbhkNTB1FgWFd+ZhC/LhRUY  
40jEiykmbEp6h1zQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt  
NTpxxcXmUKquX+pHmIkK1LKD08rNE84jqxxRsfdi6by82fjVYf2pgjJW8R1FAw+  
mL5WQRFexbfB5aXhcMo0AA==  
-----END CERTIFICATE-----" >> certificate
```

### Cape Town Region

O certificado público da AWS da região Cidade do Cabo é o seguinte:

```
$ echo "-----BEGIN CERTIFICATE-----  
MIICNjCCAZ+gAwIBAgIJAKumfZiRrnVhMA0GCSqGSib3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQOIEExBXYXNoaw5ndG9uIFN0YXR1MRAwDgYDVQOHEwdTZWF0  
dGx1MSAwHgYDVQOKExdBbWF6b24gV2ViIFNlcnPzY2VzIExmQzAgFw0xOTExmjcw  
NZEOMDVaGA8yMTk5MDUwMjA3MTQwNvowXDELMAKA1UEBhMCVVMxGTAXBgNVBAgT  
EFdhc2hpbdob24gU3RhGuxEDAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAcTF0FT  
YXpvbiBXZWIgU2VydmljZXMcgTExDMIGfMA0GCSqGSib3DQEBAQUAA4GNADCBiQKB  
gQDFd571nUzVtke3rPyRkYfv3jh0C0EMzzG72boyUNjnfw1+m0TeFratLKb9T6F  
7Tu/ZEN+vm1Yqr2+5Va8U8qlbPF0bRH+FdaKjhgwZdYXxGzQzU3ioy5W5ZM1Vyb  
7iUsxEAlxsybc3ziPYaHI42UiTkQnahmoroNeqVyhNnBpQIDAQABMA0GCSqGSib3  
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPYRVD4pAds8Guw2+krgqkY0HxLcdjosuH  
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK  
s5gbPOnokhKTMpxbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK  
-----END CERTIFICATE-----" >> certificate
```

## Milan Region

O certificado público da AWS da região Milão é o seguinte:

```
$ echo "-----BEGIN CERTIFICATE-----"  
MIICNjCCAZ+gAwIBAgIJA0Z3GEIaDcugMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTAlVTMRkwFyYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWFO  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIEzMQzAgFw0xOTEwMjQx  
NTE5MDlagA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVmxGTAXBgNVBAgT  
EFdhc2hpmd0b24gU3RhdGUxEDAObgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0FT  
YXpvbiBXZWIGU2VydmljZXMGTExDIMGFma0GCSqGSIB3DQEBAQUAA4GNADCBiQKB  
gQCjipGw3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAxjcFhWplo20+  
ivgcFCsc4AU9OpYdAph3spLey/bhHPRI1JZHRNqScKPhozsCNhKhfnzTIEQCFvSp  
DRp4zr91/Ws06/f1JFBYJ6Hhp0KwM81XQG591V6kkw07QIDAQABMA0GCSqGSIB3  
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkgUZGTT+rrMkk2n81/abzTJvsqRqGrRw  
XRKRX1KdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRh1xW1OtZkiHWCqNottz+8vpew  
wx8JGMvwotwuKB1iMsbwYRqZkFYLcvH+Opfb/Aayi20/ChQldI6M2R5VU  
-----END CERTIFICATE-----" >> certificate
```

## China Regions

O certificado público da AWS para as regiões China (Pequim) e China (Ningxia) é o seguinte.

```
$ echo "-----BEGIN CERTIFICATE-----"
MIICSzCCAbQCCQCQ97teKRD4zANBqkqhkiG9w0BAQUFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBXMHU2VhdHRSZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBjbmMuMRowGAYDVQDExF1YzIuYW1hem9uYXdzLmNvbTAe
Fw0xMzA4MjExMzIyNDNaFw0yMzA4MjExMzIyNDNaMGoxCzAJBgNVBAYTA1VTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQHQEWdTZWF0dGx1MRgwFgYDVQKQEW9B
bWF6b24uy29tIeJuYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIB3DQEBAQAA4GNADCBiQKBgQC6GFQ2WoBl1xzYH85INUMaTc4D30QXM6f+
YmWzYJD9fc7Z0UlaZIKoQATqC058KNCre+jECELEYIX56Uq0lb8LRP8tijrQ9Sp3
qJcXiH66kH0eQ4a45YdewcFOy+CSAYDU1ab6XhtQJ2r7bd4A2v3ybzbzTOWONkd0
WtgIe3M3iwIDAQABMA0GCSqGSIb3DQEBBQAA4GBAHZQC5XZVeud9GTJTsbo5AyH
ZQvkj/jfARNrD9dgBRYzzLC/NOKGW6M9wlrmks9RtdNx53nLxKq4I2Dd73gi0yQ
wY9YYwmM/LMgmp1I33Rg2Ohwq4DVgt3h0170PL6Fsgiq3dMvctsImJvjWktBQaT
bcAgaZLHGIpXPrwsA2d+
-----END CERTIFICATE-----" >> certificate
```

## GovCloud Regions

O certificado público da AWS para as regiões GovCloud da AWS é o seguinte.

```
$ echo "-----BEGIN CERTIFICATE-----"
MIIDCzCCAnSgAwIBAgIJAIe9hNq8207UMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXXNoaW5ndG9uIFN0YXR1MRAwDgYDVQHQHewdTZWF0
dGx1MSAwHgYDVQOKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZaEfow0yMTA3MTQx
NDI3NTdaFw0yNDA3MTMxNDI3NTdaMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQOIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQHQHewdTZWF0dGx1MSAwHgYDVQOKExdBbWF6
b24gV2ViIFNlcnPzY2VzIExMoZCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYE
qaIcGFfTx/SO1W5G91jHvyQdGP25n1Y91axCuOOAUTvSvNGpXrI4AXNrQF+CmIO
C4beBASnHcx082jYudWBB19Wi za0psYc9flrczSzVLmN8w/c78F/95NfiQdnUQP
pvqgcMeJo82cgHkLR7XoFWgMrZJqrcUK0gnsQcb6kakCAwEAAAoB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVROOBByEFNvW53gWJz72F5B1ZVY40/dffFYBPMIGOBgNVHSME
gYYwgYOAFNvW53gWJz72F5B1ZVY40/dffFYBPoWCKxJbcMQswCQYDVQOGEwJVUzEZ
MBcGA1UECBM0V2FzaGluz3Rvb1tDGF0ZTEQMA4GA1UEBXMHU2VhdHRSzTEgMB4G
A1UEChMXQW1hem9uIFdlyIBTZXJ2aWN1cyBMTEOCCQCHvR56vNju1DASBgNvHRM
Af8ECDAGAQH/AgeAMA0GCSqGSIB3DQEBCwUAA4GBACRkjw460GUPZCGm3/z0dIz
M2BpuH769wcOsqFzCmKEysFSK91tvtUb1osFwH4/Lb/TOPqrvtEwD1Nva5koh2
xZhNnRmDuhOhW1K9wCcnnHGRBwYst4lYL6hNV6hcrgYwGMjtjcAjBG2yMgznSNFle
Rwi/S3BFXXISixNx9cILu
```

```
-----END CERTIFICATE-----" >> certificate
```

5. Extraia a chave pública do certificado recebido do AWS Support e salve-a em um arquivo chamado *key*.

```
$ openssl x509 -pubkey -noout -in certificate >> key
```

6. Use o comando OpenSSL dgst para verificar o documento de identidade da instância.

```
$ openssl dgst -sha256 -verify key -signature signature document
```

Se a assinatura for válida, a mensagem `Verified OK` será exibida. 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.

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 e adicione-a a um novo arquivo chamado *rsa2048* junto com o cabeçalho e rodapé necessários. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

### IMDSv2

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
&& 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/
dynamic/instance-identity/rsa2048 >> rsa2048 \
&& echo "" >> rsa2048 \
&& echo "-----END PKCS7-----" >> rsa2048
```

### IMDSv1

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
&& curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048
>> rsa2048 \
&& echo "" >> rsa2048 \
&& echo "-----END PKCS7-----" >> rsa2048
```

3. Adicione o conteúdo do documento de identidade da instância dos metadados da instância a um arquivo chamado *document*. Use um dos comandos a seguir dependendo da versão do IMDS usada pela instância.

### IMDSv2

```
$ 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/
dynamic/instance-identity/document >> document
```

## IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document  
>> document
```

4. Adicione o certificado público RSA-2048 da AWS para a sua Região a um novo arquivo chamado `certificate`. Use um dos seguintes comandos dependendo da Região da instância.

### North America Regions

- Norte da Virginia

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIEejCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSib3DQEBCWUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKEdbbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNTA4MTQw  
ODU5MTJaGAy8MTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgnVBAGT  
EFdhc2hpbd0b24gU3RhdGUxEAOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbiBXZWlqU2Vydm1jZXMcTEXMDIIB1jANBgkqhkiG9w0BAQEFAOCaQ8AMiIB  
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUIapbZMFNQgRg7kTlr7Cf+gDqXKpHPjsng  
Sfnz+jHqd8WPi+pmsNs+q0Zn82Te23klmf2U52KH9/j1k8R1Ibap/yFibFTSedmegX  
E5r447GbJRsHmuIIIfZTZ/oRpui05/Vz7Soj22tdkdY2ADp7caZknxhSP915fk  
2jJMTBUOzyXUS2rBU/u1NhbTeePjcEkvzVYPAhD30TeQ+/A+uWUu89bHSQOJR8h  
Um4cFApzzgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsgYjYOY66LuFzSCXwqSnFBfv  
ffBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMASGA1UdDwQEAwIHgDAd  
BgNVHQ4EFgQUrynsPP4uqSECwy+Pi04qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUryns  
Pp4uqSECwy+Pi04qyJ8TWSmhYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX  
YXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEdbbWF6  
b24gV2ViIFNlcnPzY2VzIExMo4IJAFLfpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C  
AQAwDQYJKoZIhvCNQELBQADggEBADW/s81XijwdP6NkEoH1m9XLrvK4YTqkNfR6  
er/uRRgTx2QjFcMnrx+g87gAml1z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJm85  
haoJNAFF7EQ/zCp1EJRikLLsC7bcDL/Eriivs78/BB4RnC9W9kSp/sxd5svJmg  
N9a6FAp1pNRsWAnbP8JB1AP93oJzb1L2LQXgykTghMkQ07NaY5hg/H5o4dMPclTK  
LYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxZ0os1jV4rDjm9Q3VpA  
NWIsDEcp3GUB4proOR+C7PNkY+VGODitB0w09qBGosCBstwyEqY=  
-----END CERTIFICATE-----" >> certificate
```

- Ohio

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIEejCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSib3DQEBCWUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKEdbbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNja2MTAx  
MjU4MTThaGAy8MTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgnVBAGT  
EFdhc2hpbd0b24gU3RhdGUxEAOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbiBXZWlqU2Vydm1jZXMcTEXMDIIB1jANBgkqhkiG9w0BAQEFAOCaQ8AMiIB  
CgKCAQEA6v6kGMnRmFDLxBeqXzP4npnL65000kmQ7w8YXQygSdmNIoScGSU5wf9  
mZdcvCxCdxgALFsFqPvH8fqjE9tj0fEfzvHos8wUsIdKr0zz0MjSx3cik4tKET  
ch0EKfMnzKogDBavraCDeX1rUDU0Rg7HFqNAOr3uqDmnqtk00XC9GenS3z/7ebJ  
f1BEPAm5oYMFpX6M6St77WdNE8wEU8SuerQughimVx9kMB07imeVHBiELbMQON  
1wSWRL/61fa02keGSTfSp/0m3u+lesf2VwVFhqIJs+jbsEscPxOkIRlzy8mGd/JV  
ONb/DQpTecdUKLgXbw7Kt03HTG9iXQIDAQABo4HUMIHRMASGA1UdDwQEAwIHgDAd  
BgNVHQ4EFgQU2CTGYE5ftTjx7gQXzdZSGPEWAjY4wgY4GA1UdIwSBhjCBg4AU2CTG  
YE5fTjx7gQXzdZSGPEWAjY6hYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX  
YXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKEdbbWF6  
b24gV2ViIFNlcnPzY2VzIExMo4IJAAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C  
AQAwDQYJKoZIhvCNQELBQADggEBANDqkIpVyp2PveqUsAKke1wKCoSuw1UmH9k  
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY  
IBJcTFBbI1xBEFkZoO3wczz05+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdnB  
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fe6H1j4TBISfd03OuKzmaifQlwLYt  
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo71lp0fOT6fZ41U2xWA4+HF/89UoygZSo7  
K+cQ90xGxJ+gmlYbLFR5rbJofjrgDAb2ogbfy8LzHo2ztSe60M=
```

-----END CERTIFICATE-----" >> *certificate*

- Oregon

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIEejCCAvqgAwIBAgIJALZl3lrQCSTMMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNTA4MTQw  
OTAxMzJaGA8yMTk1MDExNza5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgnNVBAgT  
EFdhc2hpbmd0b24gU3RhdGUxEDAObgNVBActB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbIBXZWIGu2VydmljZXMGTExDIIBIjANBgkqhkiG9w0BAQEFAOCAQ8AMIIB  
CgKCAQEAA02X59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP  
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/IpzOn0Huxj38EBzmX/NdNqKm7C  
qWu1q5kmIVjKGiadfbu08wLwLcHo8ywvfgI6F1GGSe09VMC56E/hL6Cohko11LW  
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y  
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN  
fc9H9FPIFKQNBpiqfAW5Eb3La13/+wIDAQABo4HUMIHRMAsGA1UdDwQEAWIHgDAd  
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX  
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6  
b24gV2ViIFNlcnPzY2VzIExMo4IJA1Zl3lrQCSTMMA1UdEwEB/wQIMAYBAf8C  
AQAwDQYJKoZhvcNAQELBQADggEBAFZle2MnZraXCaLwEc1pW/f0oRG8nHrlPZ9W  
OYZEWbh+QanRgaikBNDtVtIwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc  
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0o1Z93FQnTrbg620K0h  
83mGCDeVKU3hLH97FYoUq+3N/IliWFhvbAYYKFJydzLhIdlCiiB99AM6Sg53rm  
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN  
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=  
-----END CERTIFICATE-----" >> certificate
```

- Norte da Califórnia

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIEejCCAvqgAwIBAgIJANNPkIpCYEtIMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNTEwMjkw  
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgnNVBAgT  
EFdhc2hpbmd0b24gU3RhdGUxEDAObgNVBActB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbIBXZWIGu2VydmljZXMGTExDIIBIjANBgkqhkiG9w0BAQEFAOCAQ8AMIIB  
CgKCAQEApHQgvHvq3SVCzdrC7575BW7GWLzcj8CLqYcl3YY7Jffupz7Ojcft057Z  
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KCh  
4TriDqr1Ii17nB5MiPJ8wTeAqX8T3SYaf6Vo+4Gcb3LCDGvnkZ9TrGcz2CHKjsj  
AIWgopFpwIjVYm7obmuIxSIUv+oNH0wXgDl029Zd98SnIYQd/njiqkzE+lvXgk  
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiIWVEyR2JKm2/iR1dL1Yst39kbNg47xY  
ar129sS4nB5W3TRQA2jLOToTlxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAWIHgDAd  
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy  
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX  
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6  
b24gV2ViIFNlcnPzY2VzIExMo4IJA1NNPkJpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C  
AQAwDQYJKoZhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E  
tNoKMI2KR81lcv8ZE1XDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9Rj4RXIDS7  
33qCQ8juF4vep2U5TTBd6hfWxt1Izi188xudjixmbpUU4YKr8UPbmixldYR+BEx0u  
B1KJi911lxvuc/Igy/xehOAZEjXzVvHp8Bne33VVwMiMxWE CZciJxE4I7+Y6fqJ  
pLLSFFJKbNaFyX1DiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYwuFVLthaBgu  
1PfHafJpj/JDcq2vKUKfur5edQ6j1CGdxqqjwahOTEqcN8m7us=  
-----END CERTIFICATE-----" >> certificate
```

- Canada (Central)

```
$ echo "-----BEGIN CERTIFICATE-----  
MIID0zCCAiogAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMoZAgFw0xNja3Mjkk  
MTM3MTdaGA8yMTk2MDExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgnNVBAgT  
EFdhc2hpbmd0b24gU3RhdGUxEDAObgNVBActB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
```

```
YXpvbiBXZWIGU2VydmljZXMcTExDMIIBIjANBgkqhkiG9w0BAQEFAOCQ8AMiIB
CgKCAQEAhDUh6j1ACSt05nSxAcwMaGr8Ez87VA2RW2Hy819XoHndnxmP50Cqld
+26AJt1tlqHpI1YdtNZ60rVgVhXcVtbvte01Z3ldEZC3PMvmISBhHs6A3SWHA9ln
InHbToLX/SWqBHLOX78HkPRaG2k0COHpry+fG9gvz8HCiQaXcbWNFDHZev9OToNI
xhXBvzIa3AgUnGMaLCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGucM00
LBvmTGGehWhi04MUZwfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJkgy4JcF8Qu3z
xxUb17Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGS1b3DQEBCwUAA4IBAQAJ
UNKm+gIIHnk0G0tzv6vZBT+o/vt+tIp81EoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl120gRWLct
rJg/K60UMXRsmg2w/cxV45pUbcyVb5h6Op5ueVAVq+Cvns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre21HLSJH5D4SdWcYqBsfpf3FQThH010KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+tTEHwRRngX7
-----END CERTIFICATE-----" >> certificate
```

## South America Regions

- São Paulo

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEejCCAvqgAwIBAgIJAMcyox4U0xxMA0GCSqGS1b3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpmdob24gU3RhGUxEADOBgNVBActB1NLYXR0bGUxIDAeBgNVBAotFOFT
YXpvbiBXZWIGU2VydmljZXMcTExDMIIBIjANBgkqhkiG9w0BAQEFAOCQ8AMiIB
CgKCAQEaw451hGZVbQcy1fHBqzRoH08Csrdzxj/WP4CrBjo/2DAnimvrCCDs5086
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPwC6EYYAnR+PLlg+aNSOGUzsyz202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJoZLm6evHuEPMAHR4/OV7hyGOiGaV/v9zqina
pmCLhbh2xk0PO35HCVBwT3HUjsgeks2eEsu9Ws6H3JXTcfiop0TjyRWapM290hA
cRjfJ/d/+wBTz1fkwoZ7TF+EWRIN5ITEad1DTnPf1r8kBGuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDDBu6oNBb2rS0K+s3QIDAQAB4HUMIHRMAsGA1UdDwQEAWIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGtwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGtYhYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnPzY2VzIExMQ4IJAmyox4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNAQELBQADggEBACoowsbf7b9AlcNr14l1r3QWWSc7k90/tUzal
PlTG3Ob12x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGxbGSCJSEjkW
VGctc/jYMHxfhx67Szmf7m/MTYnvnzsyQ03v8y3Rdah+xelNPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzzhQyyjtsrgGfTLvXeXrokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbdbhzaqlB5pCPjLLzv0zp/XmO6k+jvOePOGh
JzGk5t1Orsju+MqNPfk3+107o910Vrhqw1QRB0gr1ExrvilbyfU=
-----END CERTIFICATE-----" >> certificate
```

## Europe, Middle East, and Africa Regions

- Frankfurt

```
$ echo "-----BEGIN CERTIFICATE-----
MIIEejCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGS1b3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpmdob24gU3RhGUxEADOBgNVBActB1NLYXR0bGUxIDAeBgNVBAotFOFT
YXpvbiBXZWIGU2VydmljZXMcTExDMIIBIjANBgkqhkiG9w0BAQEFAOCQ8AMiIB
CgKCAQEAKa8FLhxS1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o/wti0cNt6MLsiUeHn15H/4U/Q/fR+GA8pJ+L
npqZDG2tF11WMvvGhGgIbScrjR4V03TuKy+rZXMyvMrk1RXZ9gPhk6evFnviwHsE
JV5AEjxLz3duD+u/Sjpplvloxe2KuWnyC+EKInnka909s14ZAUh+qIYfZK85DAjm
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISD30iZZL6VVXLXutHwVhnVASrS
ZZDVpzj+3yD5hRXsvFigGhY0FCFVfnwIDAQAB4HUMIHRMAsGA1UdDwQEAWIHgDAd
```

```
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUDn6zTuP6YcwgY4GA1UDIwSBhjCBg4AUxC21
6pvJaRflgu3MUDn6zTuP6YehYKRmfWxszAJBgnVBAyTA1VTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnPzY2VzIExMo4IJAkD+v6LeR/WrMBIGA1UDewEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNQELBQADggEBAIK+DtbUPppJXFqQMV1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5Z1MJ7Dtnr3vUkiWbV1EUaZGOU1ndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xbhF0mTKPrOGdyYmjZUtQMSVb91bMWCFfs
w+SwDLnm5NF4yZchIctS2fdpoyZpOHDXy0xg01gWhKTnYbaZOxkJvEvccKxVAwJ
obF8NyJla0/pWdjhlHafEXEN81yyxyTTyOa0BGtuYOBD2cTYynaUVKY4fqHUKr3v
Z6fboAHd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----" >> certificate
```

- Londres

```
$ echo "-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgnV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMo2AgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNT0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpbmd0b24gU3Rhdb0gNvBACtB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpzbIBXZWlgU2VydmljZXMGTExDMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCj0wpsuHE9H6dWUJy12Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWhtShzsM10JVRt+YuGetf90CPr26QmIFFs5nD4
fgsJQEr2yMBSGA9Fxq3Cw6qkWcrOpSCR+bHOu0XykdK10MnIbpBf0kTfciaUpQEA
dEHnM2J1L2i0NTLBgkxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8Txcm9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCG1YjyadQJxSz1j343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbrQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMC1gZyMMn0aQIxMigoFNgXMUNx1Mq/e/Tx+SNaOEAuOn2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRlEbBrdLqmISDnfqey8ufw0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwt09XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
h1s3170z1JQ1HzbDrH1pgp+8hSi0DwwDvb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsBqwK
-----END CERTIFICATE-----" >> certificate
```

- Paris

```
$ echo "-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgnV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMo2AgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpbmd0b24gU3Rhdb0gNvBACtB1NLYXR0bGUxIDAeBgNVBAoTF0Ft
YXpzbIBXZWlgU2VydmljZXMGTExDMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAY57KDqnEvF3drSPoFcg/oL+QYD62b1u+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SggWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPPhgK5v4330DxkQ4s+jRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIVo6kUfx0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRzyDHF6ILZu+s6ywiMicud+2U11DFC6oas+a8D11hmO/rpWU/ieV
jj4rWAfrsebpN+Nhgy96iiUVGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
iYv6FQ6knXcg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfe8GxVXqlZG1
c15WKTfDMapnb9RV/DtaVzWx3cMYT77vm1H11XGjh611CGcENH1egI31OTILsa
+kfopuJEQ9TDAIKgjhA+KieU/85Ctv9fdej6d0GC60EuWkkTNzPWue6UMq8d4H
2xqJboWsEl4nybEosvzfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiut5CYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFY
OmY0v/xVmQUQ126jJxaM
-----END CERTIFICATE-----" >> certificate
```

- Irlanda

```
$ echo "-----BEGIN CERTIFICATE-----
MIIIEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgnV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMo2AgFw0xNTEwMjkw
```

```
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOvowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbd0b24gU3RhdGUxEDAOBgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlIgU2VydmljZXmgTExDMIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAjE7nVu+aHltzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtfQR/Thvfltwu9AROVt22dUOTvERdkNzveoFCy
hf52Rqf0DmRLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP90+TpgYNT1krD5PdvJU
7HcXrkNHDYqbgs8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+Fsd6F5W+6ZSHGJ881
FI+qYKs7xsjQYgXWfEt6bckWs1kZ1a1OyMzYdPF6C1yZeeC/UhIe/uJyUUNfpT
ViSi501tBbcPF4c7Y20j0IwI2SgOOIDAQABo4HUMIHRMASGA1UdDwQEAWIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Z18mB/MxikjZDUwgY4GA1UdIwSBhjCBg4AUf2Dg
PUZivKQR/Z18mB/MxikjZDUwgY4GA1UdIwSBhjCBg4AUf2Dg
YXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWfdGx1MSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnPzY2VzIExmQ4IJAOrmqHuau0vMBIGA1UdEwEB/wgIMAYBaf8C
AQAwDQYJKoZIhvCNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1R1XTMygxXX10YggX88XPmPtok17
14hib/D9/lu4IaFIyLzYNSzsETYKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nRoOn79RcQFFhGnvup0MZ+JbljyhZUYFzC1i
31jPZiKzqWa87xh2DbAyvj2KzrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KwdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----" >> certificate
```

- Milão

```
$ echo "-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWfdGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExmQ4IJAOrmqHuau0vMBIGA1UdEwEB/wgIMAYBaf8C
AQAwDQYJKoZIhvCNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1R1XTMygxXX10YggX88XPmPtok17
14hib/D9/lu4IaFIyLzYNSzsETYKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nRoOn79RcQFFhGnvup0MZ+JbljyhZUYFzC1i
31jPZiKzqWa87xh2DbAyvj2KzrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KwdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----" >> certificate
```

- Estocolmo

```
$ echo "-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJAlc/uRg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWfdGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExmQ4IJAOrmqHuau0vMBIGA1UdEwEB/wgIMAYBaf8C
AQAwDQYJKoZIhvCNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1R1XTMygxXX10YggX88XPmPtok17
14hib/D9/lu4IaFIyLzYNSzsETYKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nRoOn79RcQFFhGnvup0MZ+JbljyhZUYFzC1i
31jPZiKzqWa87xh2DbAyvj2KzrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KwdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----" >> certificate
```

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Metadados da instância e dados do usuário

```
FExyIdEjoeO1jhTsck3R
-----END CERTIFICATE-----" >> certificate
```

- Bahrein

```
$ echo "-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xOTAyMDUX
MzA2MjBaGA8yMTk4MDcxMTEzMdYyMFowXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpbmd0b24gU3RhGUxEDAOBgNVBActB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2Vydm1jZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAY4Vnit2eBpjKgOKBmyupJzJAI4fr74tuGJNnwaa+Is2vH12jmZn9I11
UpvvEUYTiboiGSpf6SJ5LmV5rCv4jT4a1Wm0kjfnBil1kUi8SxZrPypcw24m6ke
BVuxQzrZDs+xDUYIZifTmdgD50u5YE+Tlg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIp635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKxx2dNXQ1dd
VULV+WH7s6Vm4+yBeG8ctPYH5Goo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kkt1IEhsQ+MNN29jayE5oLmtGjHj5dtA3XNklr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTuWi+Fc01JkYZxRF1VBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c50Wna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q341XZ629IyFirS5TTOICoosNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----" >> certificate
```

- Cidade do Cabo

```
$ echo "-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpbmd0b24gU3RhGUxEDAOBgNVBActB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2Vydm1jZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAY7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2w0cQdbLandh0EGtbixerete3IoXzd1KXjb11PVmrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuCNRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QwctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjjBOVbyYmtYxm/DtkprYY/e6bCAVok015X1sZDd3oCOQNoG1v5XbHJe2o
JFD8GRRy2rkWO/1NwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNIUmUjrSBOfbJsfFulyg1Zgn2nDCK7kQhx
jJMjNIVXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoY2aaXU
VEB/oQziRGyKDn1d4TGYVZHG44CkrzSDv1bfTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEE6YyE1Rak162VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU81JgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99J1
-----END CERTIFICATE-----" >> certificate
```

## Asia Pacific Regions

- Sydney

```
$ echo "-----BEGIN CERTIFICATE-----
MIIIEjCCAvqgAwIBAgIJAL2bObg+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnPzY2VzIExMQzAgFw0xNTEwMjk
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT
EFdhc2hpbmd0b24gU3RhGUxEDAOBgNVBActB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2Vydm1jZXMGTExDMMIIBiJANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dK18EYpQSeS
vz6pLhkgO4xbCRGlgE8LS/OijcZ5HwdxBiKbicR1YvIPaIyEQQvF5sX6UwkGYw
-----END CERTIFICATE-----" >> certificate
```

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Metadados da instância e dados do usuário

```
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZONW058MQ0FnEj2D7H58Ti//vFP10TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHG1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCM1S9sJ
151DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMASGA1UdDwQEAWIHgDAD
BgNVHQ4EFgQU/wHIo+r5U31ViSPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31ViSPoWoRVsNXGxoyhYKReMFwxCzAJBgnNVBAYTA1VTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6
b24gV2ViIFN1cnZpY2VzIExMo4IJAL2b0gb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNQELBQADggEBACobLvj8Ix1QyORTz/9q7/VJL509/p4HAeve
92riHp6+Mo10/dSEYPeFTgdWB9W3YCNc34SS9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElstsRSXFuVr9EawjLvhni3BaC9Ve34iP71ifr75
8TpK6PEj0+jWiijFH8E4Ghc5chB0/ooU6ioQqJrMwFyNwo1cVZJD5v6D0mu9bS
TMiJLJKv4QQQqPsNdjiB7G9bfkB6trP8UVYLHLsV1y5lGx+tgwFEYkG1N8IOO=
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBhgCN1uYo=
-----END CERTIFICATE-----" >> certificate
```

- Tóquio

```
$ echo "-----BEGIN CERTIFICATE-----
MIIIEjCCAvvgAwIBAgIJAL9KIB7Fvgv/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgnNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExMo4IJAL2b0gb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
OTAwMjVaGA8yMTk1MDExNzA5MDAYNVowXDELMakGA1UEBhMCVVMxGTAXBgnNVBAgT
EFdhc2hpbdm0b24gU3RhdGUxEADOBgNVBACTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlIgU2Vydm1jZXMGTExDMMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEa0djWUcmRW85C5CiCKPFiTIVj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gM1U+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+i
KeznOtxzq5W05NLE9bA61sziaUFNvstFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABM1TeMnvPItKOC1eRl11SsqXX1gbtl1gxSW40JWdf3WPB68E
e+/1U3F70Er7XqmNODOL6yh92Qz8fhjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rzeo90Ec51GBu13kxkWWQIDAQABo4HUMIHRMASGA1UdDwQEAWIHgDAD
BgNVHQ4EFgQU5DS1FDu/QwYbikgtWvkU3fdwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdu/QwYbikgtWvkU3fdwRihYKReMFwxCzAJBgnNVBAYTA1VTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6
b24gV2ViIFN1cnZpY2VzIExMo4IJAL9KIB7Fvgv/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvCNQELBQADggEBAG/N7ua8IE9IMy0n05T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFFt0rLOKo54pJ+Kim2cngCWNhKzctRBV567AJnt4+ZDG5
hDgVOIxW01+eaLE4qzqWP/9Vr0+p3reuumgFZLvpvVpwxBeBFUf2drUR14aWfI2
L/6VGInXYs7uP8v/2VBs7r6XZRpB0y/R4hv5efYXnjwA9gq8+a3stC2ur8m5yS1
faKSew4H320yAyaZWH4gpwUdbU1YgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoik278e/1Wqm9LrBc=
-----END CERTIFICATE-----" >> certificate
```

- Seul

```
$ echo "-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJANuCgCcHtOjhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgnNV
BAYTA1VTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExMo4IJAL2b0gb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
NTU3NDRaGA8yMTk1MDExNzE1NTc0NFowXDELMakGA1UEBhMCVVMxGTAXBgnNVBAgT
EFdhc2hpbdm0b24gU3RhdGUxEADOBgNVBACTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWlIgU2Vydm1jZXMGTExDMMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB
CgKCAQEa661Nv6pJPMGM208HbVYJS1KcAg2vUGx8xeAbzZ1QdpGfkabVcUHGB6m
Gy59VXDMD1rJckDDk6dxUOhmcX9z785TtvZURq1fua9QosdbTzX4kAgHGdp4xQEs
m06QZqg5qKjBP6xr3+Pshfq1rB8Bmwg0gXEm22CC7o7+7N7Mu2sWzWbiUR7vi14
9FjWS8XmMnwFT1Shp411TDteDWw/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105Zkj+b+K1p3adBL8OMCjgc/Pxi0+j3HQldYE
32+FaxWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQc1
mA4q+12pxy7By6g3nBk1s34PmWikNRJbwOqhf8ucGRv8aiNhRRe9lokcXomwo8r
KHbbqvtK8510xUzp/Cx4sm4aTgcMvfJP29jGLclDzeqAD1vkWEJ4+xncxSYV1s9x
+78TvF/+8h9U2LnS164PxakdxHy2IshIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy81kiOsvU9XzUaZ0fZSFxx
wXxZamQbONvFcXvHY/oPSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMr04
jmXe0aMy3thyK6g5sJVG
```

-----END CERTIFICATE-----" >> *certificate*

- Osaka

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIDOzCCAiOgAwIBAgIJAMAnlyPk22ditMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2Vi1Fn1cnZpY2VzIExMoZAgFw0xNzA3MTkx  
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgnVBAgT  
EFdhc2hpbmdb024gU3RhdGUxEDAObgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbIBXZWlIgU2VydmljZXMGTExDMMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB  
CgKCAQEArznEYef8IjhrJoaZI0QGZkm1mHm/4rEbyQbMnifxjsDE8XwtHNwaM91z  
zmyK6Sk/tKLWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsVfNBcTh/E6u+mBPH3J  
gvGanqUjt6c4IbipdEouIjjnyNyVwd4D6erL1/ENiJeR1OxVpaqSW5SBK7jms49E  
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmk1cqTfMfPCkzmJCRgp  
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzg007Z2SAE63PI048JK8HcObH  
txORUQ/XF1jzi/SiaUJZT7kq3kwl8wIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQbj  
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymqLx95v2Vj9Moxk+gJuUSR  
BzFte3TT6b3jPolbECgmAorj8NxjC17N8QAAI1d0S0gi18kqkG7V8iRyPIFekv+M  
pcail+cIV5IV5qAz8QOMGYfGdyKcoBjsgiyvMu/2N2UbZJNGWvcEGkdjGJUYYOO  
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiiUGeaW3UFEbThJT+z8UFHG9fQjzzfN/J  
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHUi1n8cbCc64MVfXe2g3EZ9Glq/9n  
izPrI09hMypJDP04ugQc  
-----END CERTIFICATE-----" >> certificate
```

- Mumbai

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmCOMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2Vi1Fn1cnZpY2VzIExMoZAgFw0xNjAzMDcx  
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVoWxDELMAkGA1UEBhMCVVMxGTAXBgnVBAgT  
EFdhc2hpbmdb024gU3RhdGUxEDAObgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbIBXZWlIgU2VydmljZXMGTExDMMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB  
CgKCAQEAOlSS5I/eCT2PM0+qusorBx67QL26BIWQhd/yF6ARtHbb/1DdFLRqE5Dj  
07Xw7eENC+T79mOxoAbeWg91KaODOzw6i9I/2/HpK0+NDEDdD6sPKDA1d45jRra+v  
CqAjI+nV9Vw91wv7HjMk3RcjWGzim8/hw+3YNIutt7aQzZRWlBpcqx3/AFd8Eu  
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+z  
w9RVHm24Bgh1LxLHLms0IxvbrF277uX9Dxu1Hfkfu5D2kimTY7xSZDNLR2dt+kNY  
/+iWd1eEPPT0PLSILT52wP6stF+3QIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQBI  
E6w+WWC2gCfoJO6c9HMyGLMFEPqZmz1n5IcQt1h9iy07Vkm1wkJiZsMhXpk73zxf  
TPxuXEacTX3SOEa070IMCFwkus05f6leOyFTyHCzBzGZ3U0ukRVZA3WcpNB6Dwy  
h7ysVlqyT9Wzd7EOYm5j5oue2G2xdei+6etgn5ujyWm61iZGrcoF6WTdmzqa6WG  
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgykIjlrbFB3pJ1OVLztIfSN5J40olpu  
JVCfIq5u1NkpzL7ys/Ub8EYipbzI6P+yxxiUSuF0v9b98ymczMYjrsQXIf1e8In3  
OP2Cc1CHoZ8XDQcvvKAh  
-----END CERTIFICATE-----" >> certificate
```

- Hong Kong

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2Vi1Fn1cnZpY2VzIExMoZAgFw0xODA3MjAw  
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgnVBAgT  
EFdhc2hpbmdb024gU3RhdGUxEDAObgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbIBXZWlIgU2VydmljZXMGTExDMMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiIB  
CgKCAQEAT1PNsOg0FDrlGlWePoHeOSmOJTA3HCRy5LsbYD33GFU2eBrOlxoU/+SM  
rInKu3GghAMFH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFTfbxF  
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOb1NWAP9BniUG0F1cz6Dp  
uPovwDTLdAYT3TyhzlohKL3f6048TR5yTaV+3Ran2SGRhJjf3FRpP4VC+z5LnT  
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401Gsm9fVA7SW3jzCGF81z  
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQDK  
2/+C3nPMyOFX/I3Cyk+Pui44IgOwCs1dNGwuJy5dqp5VIfn jegEu2zIMWJSKG0
```

```
1MZOQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+  
K8V8SzAsQDvYzs2KaE+18GFfLvf1TGUYK2rPSZMHyX-v/T1lc/qUceBycrIQ/kke  
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1  
3If8s81uTheiQjwY5t9nMOSY/1Th/tL3+RaEI79VNEvfG1FQ8mgqCK0ar4m0oZJ1  
tmmeJMJ7xeURdpBBx36Di  
-----END CERTIFICATE-----" >> certificate
```

- Cingapura

```
$ echo "-----BEGIN CERTIFICATE-----  
MIIEECJCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIECxBYXNnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEzM0zAgFw0xNTEwMjkw  
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT  
EFdhc2hpbmd0b24gU3RhGUxEDAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbiBXZWIGu2VydmljZXMGtExDMiIB1jANBgkqhkiG9w0BAQEFAOCaQ8AMIIB  
CgKCAQEAlaSSLfb170gmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEec24wd/xVy  
2RMirydGedkW4tUjkUyOyFET5OAyT43jTzDPHZTkRSVkyjBdcYbe9o/0Q4P7IVS3  
XlvwrUr0qo9nSID0mxMnOoF118KAqnn10tQ0W+1NSTkasw7QVzcb+3okPEvhPAOq  
Mn1Y3vkM0G18zX4iOKbEcSvHifZfwuiffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w  
ROg415kLYcodjgThmGPNUpAZM0C5Z4pymFuChgNAZNvzhZDA8420jecqm62zcm  
Tzh/pNMNeGCRYq2EQX0aqTyOIj7bOQIDAQAB04HUMIHRMAsGA1UdDwQEAWIHgDAD  
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB  
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTA1VTMRkwFwYDVQQIExBX  
YXNnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0dGx1MSAwHgYDVQQKExdBbWF6  
b24gV2ViIFNlcnZpY2VzIEzM04IAJAVMg5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C  
AQAwDQYJKoZIhvCNQELBQADggEBAF/0dWqkIEZKg5rc8a0P0VS+tolJJE/FRZO  
atHOeaQbWzyac6NEWjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO  
IdtJ8mAzq8CZ3ipdMs1hRqF5Grp8lg4w2QpX+PfhW47iIOBiqSAUKIr3Y3BDaDn  
EjeXF6qs4iPIvBaQQ0cvdddNh/pE33/ceghbkzNTYkrwMyBkQ1RTTVKXFN7pCRUV  
+L9FuQ9y8mPOBYza5e1sdkwebydu+eqVzsil98ntkhpjvrkaJ5+Drs8TjGaJwlRw  
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4ScVjf11z00dQ=  
-----END CERTIFICATE-----" >> certificate
```

- Ningxia

```
$ echo "-----BEGIN CERTIFICATE-----  
MIID0zCCAiOgAwIBAgIJAAPu4ssY3BlzcMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIECxBYXNnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEzM0zAgFw0xNTEyMDMy  
MTI5MzJaGA8yMTk1MDUwODIxmjkzMlowXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT  
EFdhc2hpbmd0b24gU3RhGUxEDAOBgNVBAcTB1NLYXR0bGUxIDAeBgNVBAoTF0Ft  
YXpvbiBXZWIGu2VydmljZXMGtExDMiIB1jANBgkqhkiG9w0BAQEFAOCaQ8AMIIB  
CgKCAQEAsOgi4A6+YTlZcdIyP8b8SCT2M/6PGKwzKU5XkbSBoL3gsnSwiFYqPg9c  
uJPNb1y9wSa9vlyfWmd90qvTfiNrT6vewP813QdJ3EENZox4ERcf/Wd22tV72kxD  
yw1Q3I1OMH4b0ItGQAxU5OtxCjBZEEUZooOku8RoUQOU2Pql4NTiUpzWacNutAn5  
HHS7MDc4lulsJqbN+5QW6fFrcNG/0Mrb3JbwdfUNhrQ5j+Yq5h78HarnUivnX/3  
Ap+oPbentv1qd7wvPJU556LZuhfqI0TohiIT1Ah+yUdN5osoamxTHKktf/CsSJ1F  
w3qXqFJQAOVWsqqjFyHXFI32I/GoupwIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQcN  
Um00QHvUsJSN6KATbghowLynHn2wZS0su8E0COpCFJFxP2SV0NYkERbxuOn/Vhi  
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd3z5ZgnXPb9vRkLwiMSw4uXls35  
qGraczUJ9EXDhrv7VmngIk9H3YssYr1dGEqh/oz4ze4UL0gnfkauanHikk+BUESg  
/jSTD+7e+niEZJPihHdsVKFDlud5pkEzyxovHwNJ1GS21//yxrfJFIL91mehjqEk  
RLPdNse7N6UvSnuXcOokwu616kfzigGkjbxcqc4gre3szZFdCQcUioj7Z4xtuTL8  
YMqfiDtN5cbD8R8ojw9Y  
-----END CERTIFICATE-----" >> certificate
```

- Pequim

```
$ echo "-----BEGIN CERTIFICATE-----  
MIID0zCCAiOgAwIBAgIJAAtrM5XLDSjCMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV  
BAYTA1VTMRkwFwYDVQQIECxBYXNnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0  
dGx1MSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIEzM0zAgFw0xNTA4MTQx  
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMakGA1UEBhMCVVMxGTAXBgnVBAgT
```

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Metadados da instância e dados do usuário

```
EFdhc2hpbdm0b24gU3RhGUxEDAObgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2VydmljZXMGTExdMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiB
CgKCAQEAvVBz+wQNdPiM9S+aUULQErTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LH
sgEi6+LMlCN9TwNKOToEabmDKorss4zFl7VSSbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4Obx1FN92VtvzD6QBs3CcOfWgyWGVgZ+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQa8
ezx5LRjzUU9EYWyhyYIEshFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcv7i3n+/ymQbCLC6kAg8DUB7Nt0Rll5ag8d/JXGzcTCnlDXLxx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIotbH1P+g5y113bI2leYE6Tm8
LKbyfK/532xJPq0abx4Ddn89ZEC6vvWVNDgTsxErg992Wi+/xoSw3XxkgAryIv1
zQ4dQ6irFnxWcWJqC6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGvgjM6wivVA
-----END CERTIFICATE-----" >> certificate
```

### AWS GovCloud Regions

- Região GovCloud (Oeste dos EUA) da AWS

```
$ echo "-----BEGIN CERTIFICATE-----
MIID0zCCAiOgAwIBAgIJANCOFO0Q6ohnuMA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExM0zAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMze5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbdm0b24gU3RhGUxEDAObgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2VydmljZXMGTExdMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiB
CgKCAQEAvICGtzNqie3f10lrrqcfzGfbymSM2QfbTzICG6xXXeFrCDAmQo0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvBVd4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwiy+kniFa+vXK6aQv94
1W98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMi0Y7LnkKGCIHQ/XJ
0wSiSWaCddbu59BZeADnyh14f+pWaSQpQ01DpXvZAVByvCH97J1oAxLfh8xcwgSQ
/se3wtn095Vbt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQa/
S8+a9csfASKdtQUOLSBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPk16jdF9utqZ0JUo/FxeIxm0h6oievB1SkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFByKCHws09sI+6204Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiy8GnhgWx5faCY38D/k4Y/j5Vz99
71UX/+fWHT3+lTL8ZZk7f0QWh6NQpI0wTP9KtWqfOUwM1bgFQPoxkP00TWrmmdmPz
WOWTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----" >> certificate
```

- AWSRegião GovCloud (Leste dos EUA) da

```
$ echo "-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIB3DQEBCwUAMFwxCzAJBgNV
BAYTA1VTMRkwFwYDVQQIExBXYXnoaW5ndG9uIFN0YXR1MRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFN1cnZpY2VzIExM0zAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVoWxDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbdm0b24gU3RhGUxEDAObgNVBAcTB1N1YXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIGu2VydmljZXMGTExdMIIBIjANBgkqhkiG9w0BAQEFAOCaQ8AMiB
CgKCAQEAvaxsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWApkZVxEdl2Gdhw3SULoKcKmkqE61tVfrVuPT33La1UufguT9k8ZDDuO9C
hQNHUDSVEuVrK3bLjaSsMOS7Uxmnn71YT9901ReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDQgbNzkeIblW7vK7ydsJtFMS1jga54UAVXibQt9EAIf7B8k912iLa
mu9yEjyQy+ZQ1CTuAvPUEWe6va2CHVY9gYQLA31/zU0VbKZPTNEqxjaQK4j8bKs1/
7dOV1so39s1GBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIB3DQEBCwUAA4IBAQb
hO2W/Lm+Nk0qsXW6mqQFsAou0cASC/vtGNcyBfoFNx6aKxsVChxq2aq2TUKWENs+
mKmYu11ZvhBOmLshyl1h3RRoL30hp3jCwXyt kWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMwbIr6udoD1MbsIO7+8F+jUJkh4X111Kb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1ZellpZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0Zdy19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----" >> certificate
```

-----END CERTIFICATE-----" >> *certificate*

5. Use o comando OpenSSL smime para verificar a assinatura. Inclua a opção `-verify` para indicar que a assinatura precisa ser verificada, e a opção `-noverify` para indicar que o certificado não precisa ser verificado.

```
$ openssl smime -verify -in rsa2048 -inform PEM -content document -certfile certificate  
-noverify
```

Se a assinatura for válida, a mensagem `Verification successful` será exibida. Se não for possível verificar a assinatura, entre em contato com o AWS Support.

## Amazon Elastic Inference

O Amazon Elastic Inference (EI) é um recurso que você pode associar às suas instâncias do Amazon EC2 para acelerar as workloads de inferência do Deep Learning (DL). Os aceleradores do Amazon EI vêm em vários tamanhos e são um método econômico para criar recursos inteligentes em aplicações executadas em instâncias do Amazon EC2.

O Amazon EI distribui operações de modelo definidas pelo TensorFlow, Apache MXNet e o formato Open Neural Network Exchange (ONNX) por meio do MXNet entre aceleradores de inferência de DL de baixo custo e a CPU da instância.

Para obter mais informações sobre o Amazon Elastic Inference, consulte o [Guia do desenvolvedor do Amazon EI](#).

## Identificar as instâncias do Linux do EC2

Sua aplicação pode precisar determinar se está executando em uma instância do EC2.

Para obter informações sobre como identificar as instâncias Windows, consulte [Identify EC2 Windows instances](#) (Identificar instâncias Windows do EC2) no Guia do usuário do Amazon EC2 para instâncias do Windows.

### 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. 677).

### Inspecione o UUID do sistema

Você pode obter o UUID do sistema e procurar pela presença dos caracteres "ec2" 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, para instâncias do EC2 que não estão usando o Amazon Linux 2, a implementação de distribuição do SMBIOS pode representar o UUID em formato little-endian e, portanto, os caracteres "EC2" não aparecem no início do UUID.

Example : Obter o UUID do DMI (somente AMIs HVM)

Use o seguinte comando para obter o UUID usando a Desktop Management Interface (DMI):

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

Na próxima saída de exemplo, o UUID começa com "EC2", que indica que o sistema é provavelmente uma instância do EC2.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

No exemplo de saída a seguir, o UUID é representado no formato little-endian.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Como alternativa, para instâncias criadas no sistema Nitro, você pode usar o seguinte comando:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Se a saída for um ID de instância, como a saída de exemplo a seguir, o sistema será uma instância do EC2:

```
i-0af01c0123456789a
```

Example : Obtenha o UUID do hipervisor (somente AMIs do picovolt)

Use o seguinte comando para obter o UUID do hipervisor:

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

Na próxima saída de exemplo, o UUID começa com "ec2", que indica que o sistema é provavelmente uma instância do EC2.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

# 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 \(p. 700\)](#)
- [Frota spot \(p. 749\)](#)
- [Monitorar eventos da frota usando o Amazon EventBridge \(p. 787\)](#)
- [Tutoriais para EC2 Fleet e frota spot \(p. 801\)](#)
- [Exemplo de configurações para EC2 Fleet e frota spot \(p. 812\)](#)
- [Quotas da frota \(p. 836\)](#)

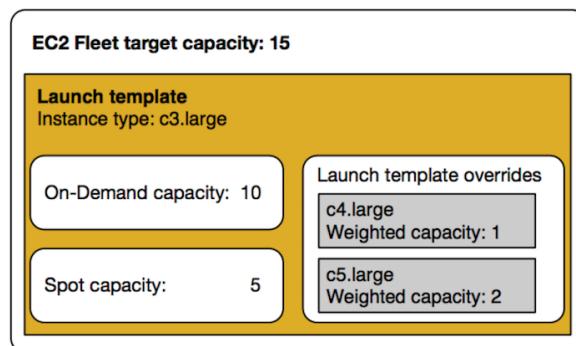
## EC2 Fleet

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 \(p. 394\)](#).



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 \(p. 701\)](#)
- [Instâncias expansíveis \(p. 701\)](#)
- [Tipos de solicitação da Frota do EC2 \(p. 702\)](#)
- [Estratégias de configuração da Frota do EC2 \(p. 720\)](#)
- [Trabalhar com Frotas do EC2 \(p. 729\)](#)

## 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 \(p. 228\)](#) 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 \(p. 245\)](#) para evitar pagar custos mais elevados. Se executar as instâncias spot expansíveis no [modo ilimitado \(p. 237\)](#) 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 \(p. 239\)](#).

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. 237) 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' \(p. 702\)](#).

`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 \(p. 721\)](#).

## 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 \(p. 731\)](#).

## 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. \(p. 739\)](#). 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 \(p. 704\)](#)

- Exemplo 2: iniciar uma única instância spot com a estratégia de alocação otimizada para capacidade (p. 705)
- Exemplo 3: iniciar uma frota spot usando pesos de instâncias (p. 707)
- Exemplo 4: iniciar instâncias spot dentro de uma única zona de disponibilidade (p. 708)
- Exemplo 5: iniciar instâncias spot de um tipo de instância único dentro de uma única zona de disponibilidade (p. 709)
- Exemplo 6: iniciar instâncias spot somente se a capacidade mínima pretendida puder ser iniciada (p. 711)
- 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. 712)
- Exemplo 8: iniciar instâncias com vários modelos de lançamento (p. 713)
- Exemplo 9: iniciar instância spot com uma base de Instâncias sob demanda (p. 715)
- 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. 716)
- Exemplo 11: iniciar instâncias spot usando a estratégia de alocação capacity-optimized-prioritized (p. 719)

#### 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 \(p. 728\)](#).

```
{  
    "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"  
                }  
            ]  
        }  
    ]  
}
```

```
        "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 \(p. 721\)](#)
- [Estratégias de alocação para Instâncias spot \(p. 721\)](#)
- [Configurar Frota do EC2 para backup sob demanda \(p. 724\)](#)
- [Rebalanceamento de capacidade \(p. 725\)](#)
- [Sobreposições de preço máximo \(p. 727\)](#)
- [Controle de gastos \(p. 727\)](#)
- [Peso de instâncias da Frota do EC2 \(p. 728\)](#)

## 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 \(p. 702\)](#).
- 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 \(p. 728\)](#).
- 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 \(p. 727\)](#).
- Leia as opções possíveis para sua Frota do EC2. Para mais informações, consulte o [Referência do arquivo de configuração JSON da Frota do EC2 \(p. 735\)](#). Para exemplos de configuração da Frota do EC2, consulte [Exemplos de configuração de Frota do EC2 \(p. 812\)](#).

## 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. 823).

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 \(p. 824\)](#).

## 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 \(p. 812\)](#), especificamente os exemplos 5 a 7.

Para obter informações sobre configuração das Reservas de Capacidade, consulte [On-Demand Capacity Reservations \(p. 481\)](#) 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 \(p. 423\)](#).

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 \(p. 822\)](#).

#### 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 \(p. 424\)](#) 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 \(p. 424\)](#) 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 \(p. 424\)](#).

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 \(p. 393\)](#).

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 \(p. 394\)](#).

## 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 \(p. 729\)](#)
- [Pré-requisitos da Frota do EC2 \(p. 731\)](#)
- [Verificações de integridade da Frota do EC2 \(p. 733\)](#)
- [Gerar um arquivo de configuração JSON da Frota do EC2 \(p. 734\)](#)
- [Criar uma Frota do EC2. \(p. 739\)](#)
- [Marcar uma Frota do EC2 \(p. 741\)](#)
- [Monitorar a Frota do EC2 \(p. 743\)](#)
- [Modificar uma Frota do EC2 \(p. 744\)](#)
- [Excluir uma Frota do EC2 \(p. 745\)](#)

## 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`.

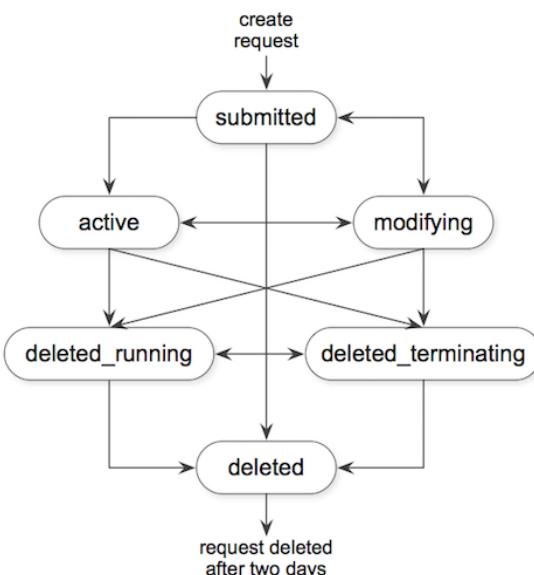
**deleted\_terminating**

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 \(p. 731\)](#)
- [Função vinculada ao serviço para Frota do EC2 \(p. 731\)](#)
- [Conceder acesso às chaves gerenciadas pelo cliente para uso com AMIs criptografadas e snapshots do EBS \(p. 732\)](#)
- [Permissões para usuários IAM da Frota do EC2 \(p. 732\)](#)

### 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 \(p. 517\)](#).

### 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 \(p. 163\)](#) ou um [snapshot do Amazon EBS criptografado \(p. 1418\)](#) 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:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "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 \(p. 841\)](#).

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. \(p. 739\)](#).
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 \(p. 721\)](#).

#### 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 \(p. 517\)](#).

#### 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 \(p. 517\)](#).

#### 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 \(gerenciar versões do modelo de inicialização\) \(p. 526\)](#).

#### 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 \(p. 702\)](#).

#### 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 \(p. 519\)](#). Para obter informações sobre marcação após a execução, consulte [Marcar com tag os recursos do \(p. 1553\)](#).

## 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 \(p. 735\)](#).

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 \(p. 812\)](#).

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 \(p. 1552\)](#).

### 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 \(p. 734\)](#) 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 \(p. 519\)](#) 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-73fbcd2ce-aa30-494c-8788-1cee4EXAMPLE \
--terminate-instances
```

A seguir está um exemplo de saída.

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbcd2ce-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-73fbcd2ce-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-qnDLWs6JLFd  
KnSMMiq5s6cGqjjPtEDpsnGHzyHasFHOaRYJpaDVravow25azn6KNkUQqlFwhJyujt2dtNCdduJfrqcFYAjleEiRMkfDht7N63SKlw-  
BHTurzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVhbY9JhLvGypLcMuJtJ76H9ytg2zR-  
VPiU5v2s-  
UgZ7h0p2yth6ysUdh1ONG6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-  
EMhekLFZeJLr  
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXXWVywzgnLtHeRf2o4lUhGBw17mXss07k7XAfdpPM-  
PT9vrHtQiILor5VVTsjSPWg7edj__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 \(p. 749\)](#)
- [Estratégias de configuração de frota spot \(p. 749\)](#)
- [Trabalhar com frotas spot \(p. 757\)](#)
- [Métricas do CloudWatch para frota spot \(p. 778\)](#)
- [Escalabilidade automática para frota spot \(p. 780\)](#)

## 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 \(console\) \(p. 765\)](#).

Os dois tipos de solicitações se beneficiam com a estratégia de alocação. Para obter mais informações, consulte [Estratégia de alocação para Instâncias spot \(p. 750\)](#).

## 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 \(p. 750\)](#)
- [Estratégia de alocação para Instâncias spot \(p. 750\)](#)
- [Sob demanda na frota spot \(p. 753\)](#)
- [Rebalanceamento de capacidade \(p. 753\)](#)
- [Substituições do preço spot \(p. 755\)](#)
- [Controle de gastos \(p. 755\)](#)
- [Peso de instâncias de frotas spot \(p. 756\)](#)

## 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 \(p. 756\)](#).
- 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 \(p. 825\)](#).

## 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 \(p. 835\)](#).

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 \(p. 835\)](#).

## 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 \(p. 423\)](#).

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 \(console\) \(p. 765\)](#).
- 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 \(p. 834\)](#).

### 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 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 \(p. 424\)](#) 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 \(p. 424\)](#) 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 \(p. 424\)](#).

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 \(p. 393\)](#).

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 \(p. 394\)](#).

## 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 \(p. 758\)](#)

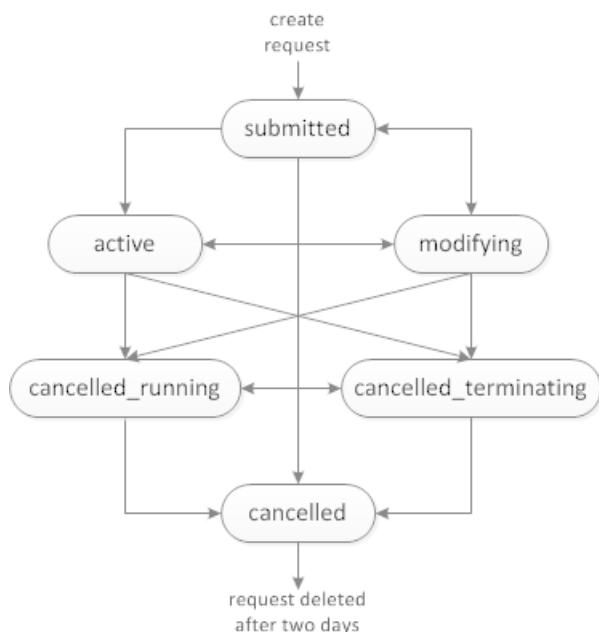
- Verificações de integridade da frota spot (p. 759)
  - Permissões de frota spot (p. 759)
  - Criar uma solicitação de frota spot (p. 764)
  - Marcar uma frota spot (p. 768)
  - Monitorar sua frota spot (p. 775)
  - Modificar uma solicitação de frota spot (p. 775)
  - Cancelar uma solicitação de frota spot (p. 777)

## 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 \(p. 841\)](#).

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 \(console\) \(p. 765\)](#).
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 \(p. 768\)](#).
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 \(p. 760\)](#)
- [Função vinculada ao serviço para frota spot \(p. 762\)](#)
- [Função vinculada ao serviço para instâncias spot \(p. 763\)](#)
- [Função do IAM para marcar uma frota spot \(p. 764\)](#)

### 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 \(p. 163\)](#) ou um [snapshot criptografado do Amazon EBS \(p. 1418\)](#) 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 \(p. 763\)](#).

### 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 \(p. 163\)](#) ou um [snapshot do Amazon EBS criptografado \(p. 1418\)](#) 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 \(p. 401\)](#).

## 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 \(p. 768\)](#).

### 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 \(console\) \(p. 764\)](#). Caso contrário, você pode modificar qualquer uma das configurações padrão. Para obter mais informações, consulte [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 765\)](#) e [Criar uma frota spot usando a AWS CLI \(p. 768\)](#).

Opções para criar uma frota spot

- [Criar uma solicitação de frota spot rapidamente \(console\) \(p. 764\)](#)
- [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 765\)](#)
- [Criar uma frota spot usando a AWS CLI \(p. 768\)](#)

## 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 \(p. 753\)](#).

#### 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 \(p. 755\)](#).

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 \(p. 750\)](#).

- 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 \(p. 825\)](#).

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 \(p. 1552\)](#).

#### Tópicos

- [Prerequisite \(p. 769\)](#)
- [Marcar uma nova frota spot \(p. 770\)](#)
- [Marcar uma nova frota spot e as instâncias e os volumes que ela executa \(p. 771\)](#)
- [Marcar uma frota spot existente \(p. 773\)](#)
- [Exibir tags de solicitações de frota spot \(p. 774\)](#)

## 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 \(console\) \(p. 765\)](#).
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 \(console\) \(p. 765\)](#).

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 \(p. 519\)](#) que é referenciado na solicitação de frota spot.

Tags de volume:

- Especifique as tags para os volumes no [modelo de execução \(p. 519\)](#) 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 \(p. 519\)](#) 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 \(p. 519\)](#) 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 \(p. 873\)](#).

Para obter mais informações sobre as métricas do CloudWatch fornecidas pelo Amazon EC2, consulte [Monitorar instâncias usando o CloudWatch \(p. 872\)](#).

## 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 \(p. 876\)](#).

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 \(p. 782\)](#): 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 \(p. 783\)](#): 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 \(p. 785\)](#): aumenta ou diminui a capacidade atual da frota com base em data e hora.

Se estiver usando [peso da instância \(p. 756\)](#), 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 \(p. 873\)](#) e [Criar uma solicitação de frota spot usando parâmetros definidos \(console\) \(p. 765\)](#).

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 \(p. 760\)](#) 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 adicioná-la 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 -infinito 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 +infinito. 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 \(p. 787\)](#)
- [Tipos de evento de frota spot \(p. 791\)](#)
- [Criar uma regra do Amazon EventBridge \(p. 796\)](#)

## 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 \(p. 788\)](#)
- [Alteração da solicitação de instância spot da EC2 Fleet \(p. 789\)](#)
- [Alteração da instância da EC2 Fleet \(p. 789\)](#)
- [Informações da EC2 Fleet \(p. 790\)](#)
- [Erro de EC2 Fleet \(p. 791\)](#)

## 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-01234567890123456",  
        "state": "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 \(p. 792\)](#)
- [Alteração da solicitação de instância spot da frota spot do EC2 \(p. 793\)](#)
- [Alteração da instância da frota spot do EC2 \(p. 794\)](#)
- [Informações sobre a frota spot do EC2 \(p. 794\)](#)
- [Erro na frota spot do EC2 \(p. 795\)](#)

## 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 \(p. 796\)](#)
- [Use o Amazon EventBridge para monitorar eventos de frota spot \(p. 799\)](#)

## 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” \(p. 787\)](#).

#### Exemplos

- [Criar uma regra de EventBridge para enviar uma notificação \(p. 797\)](#)
- [Criar uma regra de EventBridge para acionar uma função do Lambda \(p. 798\)](#)

### 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” \(p. 791\)](#).

### Exemplos

- [Criar uma regra de EventBridge para enviar uma notificação \(p. 797\)](#)
- [Criar uma regra de EventBridge para acionar uma função do Lambda \(p. 798\)](#)

## 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 \(p. 802\)](#)
- [Tutorial: Utilizar a Frota do EC2 com a opção sob demanda como a capacidade principal \(p. 804\)](#)
- [Tutorial: Inicie Instâncias sob demanda usando Reservas de Capacidade direcionadas \(p. 805\)](#)
- [Tutorial: Usar frota spot com ponderação de instâncias \(p. 810\)](#)

## 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 \(p. 731\)](#).

## 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 \(p. 519\)](#).

## 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. \(p. 739\)](#).

## 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 \(p. 731\)](#).

## 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 \(p. 519\)](#).

## 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. \(p. 739\)](#).

## 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 \(p. 806\)](#)
- [Etapa 2: Criar um grupo de recursos de Reservas de capacidade \(p. 807\)](#)
- [Etapa 3: Adicionar as Reservas de Capacidade ao grupo de recursos Reservas de Capacidade \(p. 807\)](#)
- [\(Opcional\) Etapa 4: Exibir Reservas de Capacidade no grupo de recursos \(p. 807\)](#)
- [Etapa 5: Criar um modelo de inicialização que especifique que a Reserva de capacidade se destina a um grupo de recursos específico \(p. 808\)](#)
- [\(Opcional\) Etapa 6: Descrever o modelo de inicialização \(p. 808\)](#)
- [Etapa 7: Criar uma frota EC2 \(p. 809\)](#)
- [\(Opcional\) Etapa 8: Exibir o número de Reservas de Capacidade não utilizadas restantes \(p. 810\)](#)

## 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 \(p. 724\)](#).

```
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 \(p. 759\)](#).

## 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": "r3.2xlarge",
"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 \(p. 749\)](#).

## 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 \(p. 812\)](#)
- [Exemplos de configuração de frota spot \(p. 825\)](#)

## 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 \(p. 735\)](#).

### Exemplos

- [Exemplo 1: Executar Instâncias spot como a opção de compra padrão \(p. 813\)](#)
- [Exemplo 2: Executar Instâncias on-demand como a opção de compra padrão \(p. 813\)](#)
- [Exemplo 3: Executar Instâncias on-demand como a capacidade principal \(p. 814\)](#)
- [Exemplo 4: Iniciar Instâncias spot usando a estratégia de alocação lowest-price \(p. 814\)](#)
- [Exemplo 5: Iniciar Instâncias sob demanda usando várias Reservas de Capacidade \(p. 815\)](#)
- [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 \(p. 817\)](#)
- [Exemplo 7: Iniciar Instâncias sob demanda usando Reservas de Capacidade direcionadas \(p. 820\)](#)
- [Exemplo 8: Configurar o rebalanceamento de capacidade para executar a Instâncias spot de substituição \(p. 822\)](#)
- [Exemplo 9: iniciar instâncias spot em uma frota otimizada para capacidade \(p. 823\)](#)
- [Exemplo 10: iniciar instâncias spot em uma frota otimizada para capacidade com prioridades \(p. 824\)](#)

## 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 não utilizadas disponíveis.
- 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 \(p. 805\)](#).

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",  
        "MaxLaunchRate": 10,  
        "LaunchTemplateConfigs": [  
            {  
                "LaunchTemplateSpecification": {  
                    "LaunchTemplateName": "my-launch-template",  
                    "Version": "1"  
                },  
                "Overrides": [  
                    {  
                        "InstanceType": "c5.xlarge",  
                        "AvailabilityZone": "us-east-1a"  
                    },  
                    {  
                        "InstanceType": "c5.xlarge",  
                        "AvailabilityZone": "us-east-1b"  
                    }  
                ]  
            }  
        ]  
    }  
}
```

```
"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 \(p. 725\)](#).

```
{  
    "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 \(p. 764\)](#).

### 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 \(p. 826\)](#)
- [Exemplo 2: executar Instâncias spot usando a zona de disponibilidade ou a sub-rede de menor preço de uma lista especificada \(p. 826\)](#)
- [Exemplo 3: executar Instâncias spot usando o tipo de instância de menor preço de uma lista especificada \(p. 828\)](#)
- [Exemplo 4: Cancelar o preço da solicitação \(p. 829\)](#)
- [Exemplo 5: executar uma frota spot usando a estratégia de alocação diversificada \(p. 830\)](#)
- [Exemplo 6: executar uma frota spot usando o peso da instância \(p. 832\)](#)
- [Exemplo 7: executar uma frota spot com capacidade sob demanda \(p. 833\)](#)

- 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. 835)

## 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 \(p. 750\)](#).

### 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 \(p. 756\)](#).

### 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 \(p. 753\)](#).

```
{
    "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 \(p. 753\)](#).

```
{
    "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",
                    "Priority": 1
                    "AvailabilityZone": "us-west-2a"
                },
                {
                    "InstanceType": "m4.2xlarge",
                    "Priority": 2
                    "AvailabilityZone": us-west-2b
                },
                {
                    "InstanceType": "c5.2xlarge",
                    "Priority": 3
                    "AvailabilityZone": us-west-2b
                }
            ]
        }
    ]
}
```

## 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 \(p. 438\)](#) e [limites de volume \(p. 1520\)](#). 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.

# 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	<a href="#">CPUUtilization (p. 875)</a>	
Utilização da rede	<a href="#">NetworkIn (p. 875)</a> <a href="#">NetworkOut (p. 875)</a>	
Performance do disco	<a href="#">DiskReadOps (p. 875)</a> <a href="#">DiskWriteOps (p. 875)</a>	
Leituras/gravações de disco	<a href="#">DiskReadBytes (p. 875)</a> <a href="#">DiskWriteBytes (p. 875)</a>	
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] <a href="#">Colecionar métricas e logs das instâncias do Amazon EC2 e servidores locais com o agente do CloudWatch</a> [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] <a href="#">Migrar coleção de logs da instância Windows Server para o agente do CloudWatch</a>

## 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 \(p. 839\)](#)
- [Ferramentas de monitoramento manual \(p. 840\)](#)

## 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 \(p. 841\)](#).

- 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 \(p. 841\)](#).

- 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 \(p. 872\)](#).

- 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 para Microsoft System Center](#).

## 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 \(p. 841\)](#)
- [Eventos programados para instâncias \(p. 848\)](#)

## 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 \(p. 882\)](#). 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 \(p. 846\)](#).

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 \(p. 593\)](#).

#### Tópicos

- [Tipos de verificações de status \(p. 842\)](#)
- [Visualizar verificações de status \(p. 843\)](#)
- [Relatar status da instância \(p. 845\)](#)
- [Criar e editar alarmes de verificação de status \(p. 846\)](#)

## 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
- Kernel incompatível

#### 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 an EC2 instance. At the top, there is a table listing three instances. The first instance, 'i-0c0186a12aab3741d', has a checked checkbox and is highlighted. Below the table, a modal window titled 'Instance: i-0c0186a12aab3741d' is open, specifically showing the 'Status checks' tab. This tab displays a table of system status checks. One check, 'System reachability check passed', is shown in green. Another check, 'Instance reachability check failed', is shown in red with a note indicating a failure at 2020/12/16 17:30 GMT+2 (about 1 month). At the bottom of the modal, there are buttons for 'Open support case' and 'Visit the Support Center or post a question to the Discussion Forums'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Avail
<input checked="" type="checkbox"/> -	i-0c0186a12aab3741d	<span>Running</span>	t2.large	<span>△ 1/2 checks ...</span>	No alarms	eu-w
<input type="checkbox"/> -	i-0138edcaf722db475	<span>Running</span>	m4.large	<span>○ 2/2 checks ...</span>	No alarms	eu-w
<input type="checkbox"/> -	i-02c65b735153975ec	<span>Running</span>	t3.medium	<span>○ 2/2 checks ...</span>	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	Instance status checks
<span>○ System reachability check passed</span>	<span>✗ Instance reachability check failed</span>
	Check failure at 2020/12/16 17:30 GMT+2 (about 1 month)

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](#)

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. Para resolver falhas de verificação de status de instância ou sistema, consulte [Solução de problemas em instâncias com falha nas verificações de status \(p. 1586\)](#).

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 navigation bar. Below it, there are two sections: 'System Status Checks' and 'Instance Status Checks'. The 'System Status Checks' section contains a single item: 'System reachability check passed'. The 'Instance Status Checks' section contains a single item: 'Instance reachability check failed at October 7, 2013 11:52:11 AM UTC+2 (16 minutes ago)'. There is also a note below stating '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. Para resolver falhas de verificação de status de instância ou sistema, consulte [Solução de problemas em instâncias com falha nas verificações de status \(p. 1586\)](#).

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)

Se houver uma instância com uma verificação de status com falha, consulte [Solução de problemas em instâncias com falha nas verificações de status \(p. 1586\)](#).

## 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 \(p. 882\)](#) 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 \(p. 849\)](#)

- [Visualizar eventos agendados \(p. 849\)](#)
- [Personalizar notificações de eventos programados \(p. 853\)](#)
- [Trabalhar com instâncias programadas para interrupção ou retirada \(p. 855\)](#)
- [Trabalhar com instâncias programadas para reinicialização \(p. 856\)](#)
- [Trabalhar com instâncias programadas para manutenção \(p. 857\)](#)
- [Reagendar um evento programado \(p. 858\)](#)
- [Definir janelas de eventos para eventos programados \(p. 860\)](#)

## 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)						
Resource ID		Event status	Event type	Description	Progress	Duration
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
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 four columns: '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 \(p. 649\)](#) 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 \(p. 649\)](#) 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 \(p. 853\)](#)
- [Remover tags de notificações de eventos \(p. 854\)](#)
- [Visualizar as tags a serem incluídas nas notificações de eventos \(p. 855\)](#)

## 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 \(p. 584\)](#).

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 \(p. 562\)](#).

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 \(p. 858\)](#) para que a instância seja reinicializada em uma data e hora específicas que sejam adequadas para você.

Se você interromper sua [instância do EC2 \(p. 1112\)](#) 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 \(p. 858\)](#) a reinicialização da instância para uma data e hora que sejam adequadas para você ou [reiniciar \(p. 583\)](#) 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 \(p. 858\)](#) 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 \(p. 562\)](#).

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 \(p. 859\)](#).

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 \(p. 860\)](#)
- [Visualizador de eventos do Windows \(p. 861\)](#)
- [Criar janelas de eventos \(p. 863\)](#)
- [Modificar janelas de \(p. 866\)](#)
- [Excluir janelas de eventos \(p. 871\)](#)
- [Marcar janelas de eventos \(p. 871\)](#)

## 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 \(p. 858\)](#).
- 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 \(p. 860\)](#) 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": {  
        "InstanceEventWindowId": "iew-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": {  
        "InstanceEventWindowId": "iew-0abcdef1234567890",  
        "Name": "myEventWindowName",  
        "TimeRanges": [  
            {  
                "StartWeekDay": "monday",  
                "StartHour": 21,  
                "EndWeekDay": "wednesday",  
                "EndHour": 23  
            }  
        ]  
    }  
}
```

```
        "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 `--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 `--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](#) especifica 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](#) especifica 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 \(p. 863\)](#).

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 \(p. 873\)](#).

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 \(p. 873\)](#)
- [Listar as métricas disponíveis do CloudWatch para as instâncias \(p. 875\)](#)
- [Obter estatísticas para as métricas das instâncias \(p. 888\)](#)
- [Representar métricas em gráficos para as instâncias \(p. 896\)](#)
- [Criar um alarme do CloudWatch para uma instância \(p. 896\)](#)
- [Criar alarmes para interromper, encerrar, reiniciar ou recuperar uma instância \(p. 898\)](#)

## 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 <a href="#">página de definição de preço de Amazon CloudWatch</a> .

### Tópicos

- [Permissões obrigatórias do IAM \(p. 873\)](#)
- [Habilitar o monitoramento detalhado \(p. 873\)](#)
- [Desativar o monitoramento detalhado \(p. 874\)](#)

## 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 \(p. 1477\)](#).

### 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 \(p. 888\)](#).

#### Tópicos

- [Métricas de instância \(p. 876\)](#)
- [Métricas de crédito de CPU \(p. 878\)](#)
- [Métricas de Host Dedicado \(p. 880\)](#)
- [Métricas do Amazon EBS para instâncias baseadas em Nitro \(p. 880\)](#)
- [Métricas de verificação de status \(p. 882\)](#)
- [Métricas de espelhamento de tráfego \(p. 883\)](#)
- [Dimensões de métrica do Amazon EC2 \(p. 883\)](#)
- [Métricas de uso do Amazon EC2 \(p. 884\)](#)
- [Listar métricas usando o console \(p. 885\)](#)
- [Listar métricas usando o AWS CLI \(p. 887\)](#)

## 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 <a href="#">Transição para usar o Serviço de metadados da instância versão 2 (p. 652)</a>.</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 <code>for Sum (Soma)</code>, divida esse número por 300 para encontrar o número de bytes/segundo. Se você tiver o monitoramento detalhado (1 minuto) e a estatística <code>for Sum (soma)</code>, 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 <code>Sum (soma)</code> 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 <code>Sum (soma)</code> 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. 228).

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"><li>• 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.</li><li>• A instância é interrompida ou encerrada.</li><li>• A instância é alterada de <code>unlimited</code> para <code>standard</code>.</li></ul> <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 \(p. 210\)](#).

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 <a href="#">Otimizadas para EBS por padrão (p. 1439)</a>: 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 <a href="#">Otimizadas para EBS por padrão (p. 1439)</a>: 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 \(p. 1477\)](#). Para obter informações sobre as métricas fornecidas para suas frotas Spot, consulte [Métricas do CloudWatch para frota spot \(p. 778\)](#).

## 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 \(p. 841\)](#).

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 &amp; 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. At the top, there are three tabs: 'All metrics' (selected), '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 and their metric counts:

722 Metrics	
EBS	117 Metrics
EFS	7 Metrics
ElasticBeanstalk	8 Metrics
S3	4 Metrics
EC2	316 Metrics
ELB	210 Metrics
RDS	60 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 \(p. 888\)](#)
- [Obter estatísticas para uma instância específica \(p. 888\)](#)
- [Aregar estatísticas entre instâncias \(p. 892\)](#)
- [Aregar estatísticas por grupo de Auto Scaling \(p. 894\)](#)
- [Aregar estatísticas por AMI \(p. 895\)](#)

## 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 \(p. 873\)](#).

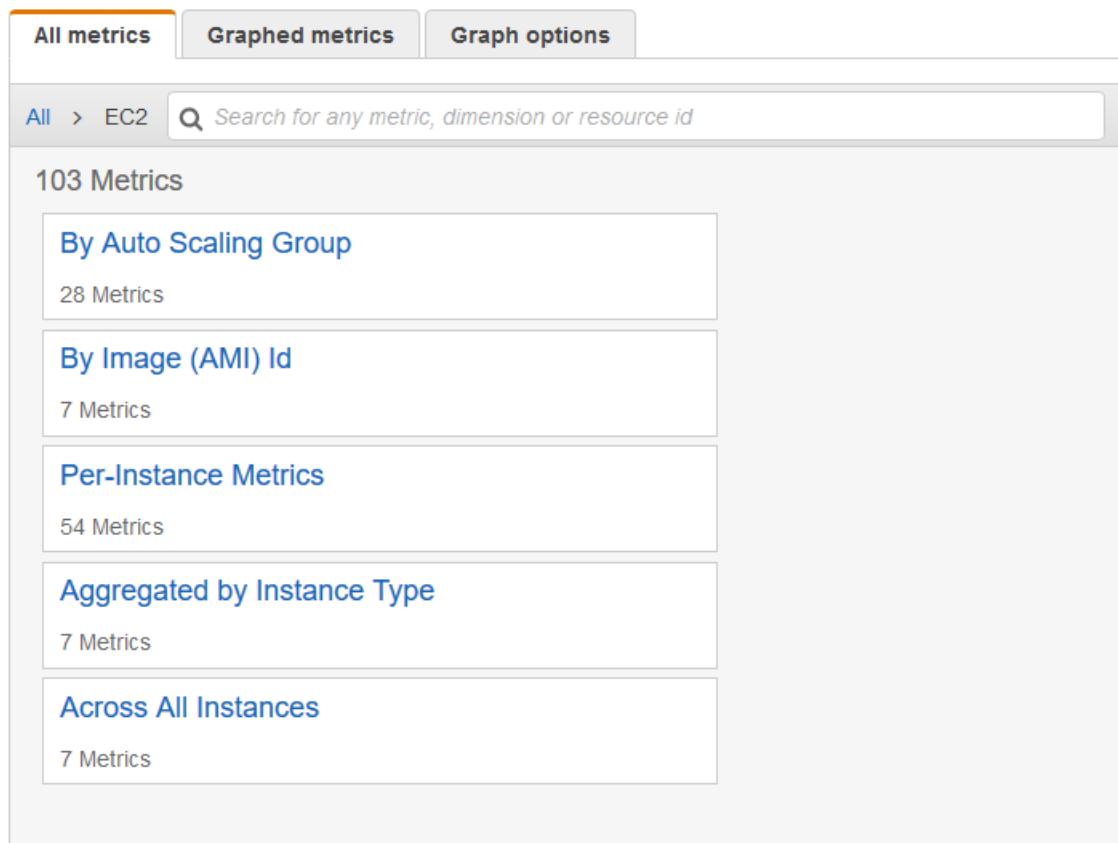
Para exibir a utilização de CPU para uma instância específica (console)

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.

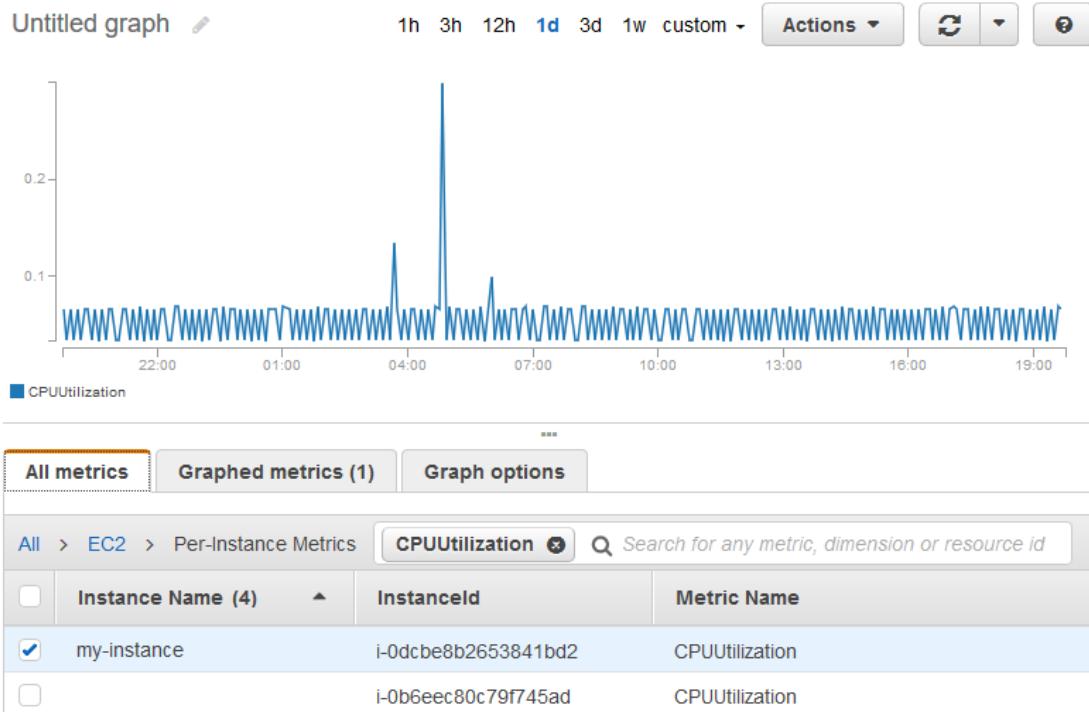
The screenshot shows the AWS CloudWatch Metrics console interface. At the top, there are three tabs: "All metrics", "Graphed metrics" (which is highlighted in orange), and "Graph options". Below the tabs is a search bar with the placeholder text "Search for any metric, dimension or resource id". The 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).



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.

Label	Namespace	Dimensions	Metric Name	Statistic	Period
CPUUtilization	EC2	Dimensions (1)	CPUUtilization	Average	<div style="display: inline-block; vertical-align: middle; text-align: right; margin-right: 10px;"> <span style="font-size: small;">1 Minute</span>  <span style="font-size: small;">5 Minutes</span>  <span style="font-size: small;">15 Minutes</span>  <span style="font-size: small;">1 Hour</span>  <span style="font-size: small;">6 Hours</span>  <span style="font-size: small;">1 Day</span> </div>

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 \(p. 873\)](#) (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.

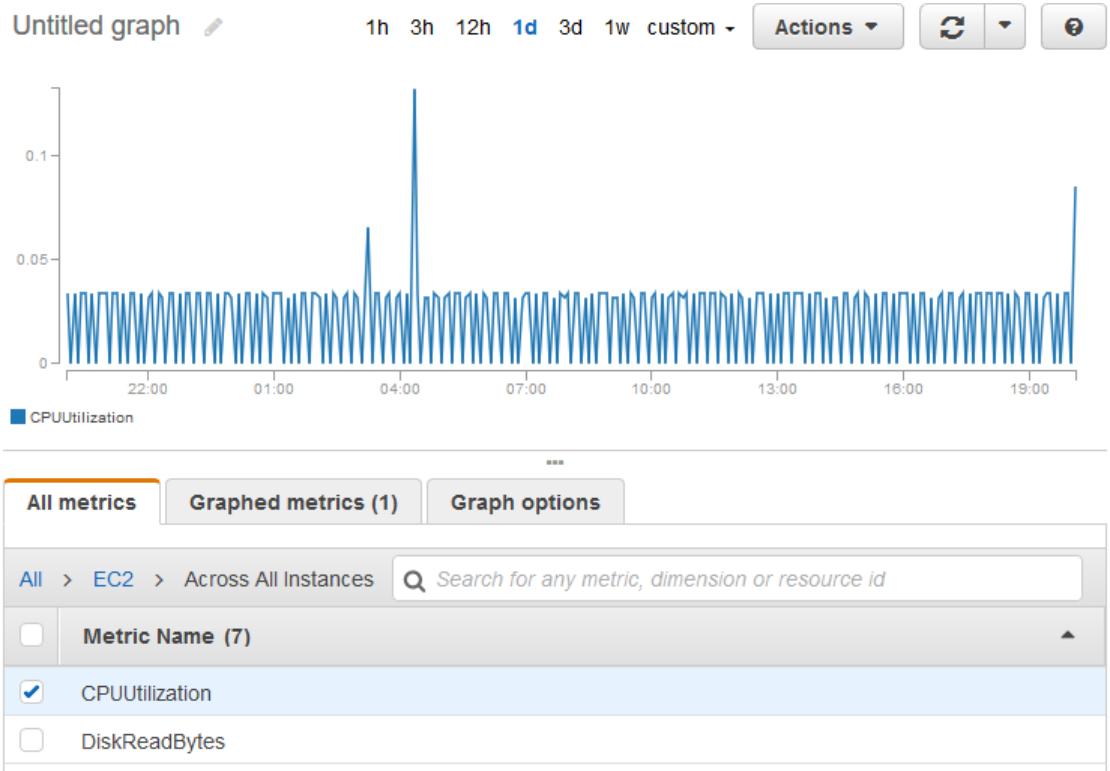
Este exemplo mostra a você como usar o monitoramento detalhado para obter uso médio de CPU para suas instâncias do EC2. Como nenhuma dimensão é especificada, o CloudWatch retorna estatísticas para todas as dimensões no namespace AWS/EC2.

### 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).



- 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 \(p. 873\)](#) (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 \(p. 875\)](#).

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.

**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:** my-topic [cancel](#)

**With these recipients:** me@mycompany.com

**Take the action:**  Recover this instance [i](#)  
 Stop this instance [i](#)  
 Terminate this instance [i](#)  
 Reboot this instance [i](#)

**Whenever:** Average of CPU Utilization

**Is:**  $\geq$  80 Percent

**For at least:** 1 consecutive period(s) of 5 Minutes

**Name of alarm:** CPU-Utilization

[Cancel](#) [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 \(p. 899\)](#)
- [Adicionar ações de encerramento a alarmes do Amazon CloudWatch \(p. 901\)](#)
- [Adicionar ações de reinicialização a alarmes do Amazon CloudWatch \(p. 902\)](#)
- [Adicionar ações de recuperação a alarmes do Amazon CloudWatch \(p. 904\)](#)
- [Usar o console do Amazon CloudWatch para visualizar o histórico do alarme e da ação \(p. 906\)](#)
- [Cenários de ação do alarme do Amazon CloudWatch \(p. 907\)](#)

## 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 escolha 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 \(p. 589\)](#).

### 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 \(p. 583\)](#).

#### 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 uma 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: A1, C3, C4, C5, C5a, C5n, C6g, C6gn, Inf1, M3, M4, M5, M5a, M5n, M5zn, M6g, M6i, P3, R3, R4, R5, R5a, R5b, R5n, R6g, T2, T3, T3a, T4g, 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 toggle switch  
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 toggle switch  
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** ▼ **5** ▼  
Consecutive Period **6** ▼ Period **7** minutes ▼  
Alarm name 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	$\leq$
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	$\leq$

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](#).

## Monitorar métricas de memória e de disco para instâncias do Linux do Amazon EC2

É possível usar o Amazon CloudWatch para coletar métricas e logs de sistemas operacionais para suas instâncias do EC2.

### Important

Os scripts de monitoramento do CloudWatch estão obsoletos. Recomendamos que você use o agente do CloudWatch para coletar métricas e logs. Para obter mais informações, consulte [Coletar métricas de instâncias do Amazon EC2 e de servidores no local com o agente do CloudWatch](#) no Guia do usuário do Amazon CloudWatch.

Se você ainda estiver migrando de scripts de monitoramento obsoletos para o agente e exigir informações sobre os scripts de monitoramento, consulte [Obsoleto: coletar métricas usando os scripts de monitoramento do CloudWatch \(p. 911\)](#).

## Coletar métricas usando o agente do CloudWatch

É possível usar um agente do CloudWatch para coletar métricas do sistema e arquivos de log das instâncias do Amazon EC2 e de servidores no local. O agente oferece suporte ao Windows Server e ao Linux e permite que você selecione as métricas a serem coletadas, incluindo métricas de sub-recurso como núcleo por CPU. Recomendamos usar o agente para coletar métricas e logs em vez de usar os scripts de monitoramento obsoletos. Para obter mais informações, consulte [Coletar métricas de instâncias do Amazon EC2 e de servidores no local com o agente do CloudWatch](#) no Guia do usuário do Amazon CloudWatch.

## Obsoleto: coletar métricas usando os scripts de monitoramento do CloudWatch

### Important

Os scripts de monitoramento do CloudWatch estão obsoletos. Fornecemos informações sobre os scripts de monitoramento para clientes que ainda não migraram dos scripts de monitoramento obsoletos para o agente do CloudWatch.

Recomendamos que você use o agente do CloudWatch para coletar métricas e logs. Para obter mais informações, consulte [Coletar métricas de instâncias do Amazon EC2 e de servidores no local com o agente do CloudWatch](#) no Guia do usuário do Amazon CloudWatch.

Os scripts de monitoramento demonstram como produzir e consumir métricas personalizadas para o Amazon CloudWatch. Esses scripts Perl de amostra formam um exemplo totalmente funcional que relata métricas de utilização de memória, swap e espaço em disco para uma instância do Linux.

Aplicam-se cobranças de uso padrão do Amazon CloudWatch para métricas personalizadas para seu uso desses scripts. Para obter mais informações, consulte a página de definição de preços do [Amazon CloudWatch](#).

### Tópicos

- [Sistemas compatíveis \(p. 912\)](#)
- [Permissões obrigatórias \(p. 912\)](#)
- [Instalar os pacotes obrigatórios \(p. 912\)](#)
- [Instalar scripts de monitoramento \(p. 914\)](#)
- [mon-put-instance-data.pl \(p. 914\)](#)
- [mon-get-instance-stats.pl \(p. 917\)](#)
- [Visualizar as métricas personalizadas no console \(p. 919\)](#)
- [Troubleshoot \(p. 919\)](#)

## Sistemas compatíveis

Os scripts de monitoramento foram testados em instâncias usando os seguintes sistemas. O uso dos scripts de monitoramento em qualquer outro sistema operacional não é permitido.

- Amazon Linux 2
- Amazon Linux AMI 2014.09.2 e posterior
- Red Hat Enterprise Linux 6.9 e 7.4
- SUSE Linux Enterprise Server 12
- Ubuntu Server 14.04 e 16.04

## Permissões obrigatórias

Certifique-se de que os scripts tenham permissão para chamar as seguintes ações associando uma função do IAM à instância:

- cloudwatch:PutMetricData
- cloudwatch:GetMetricStatistics
- cloudwatch>ListMetrics
- ec2:DescribeTags

Para obter mais informações, consulte [Trabalhar com funções do IAM \(p. 1198\)](#).

## Instalar os pacotes obrigatórios

Com algumas versões do Linux, é necessário instalar módulos Pearl adicionais antes de poder usar os scripts de monitoramento.

Para instalar os pacotes necessários no Amazon Linux 2 e na AMI do Amazon Linux

1. Iniciar a sessão na sua instância. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. Em um prompt de comando, instale pacotes da forma a seguir:

```
sudo yum install -y perl-Switch perl-DateTime perl-Sys-Syslog perl-LWP-Protocol-https  
perl-Digest-SHA.x86_64
```

Como instalar os pacotes necessários em Ubuntu

1. Iniciar a sessão na sua instância. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).

- 
2. Em um prompt de comando, instale pacotes da forma a seguir:

```
sudo apt-get update
sudo apt-get install unzip
sudo apt-get install libwww-perl libdatetime-perl
```

Como instalar os pacotes necessários no Red Hat Enterprise Linux 7

1. Iniciar a sessão na sua instância. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. Em um prompt de comando, instale pacotes da forma a seguir:

```
sudo yum install perl-Switch perl-Datetime perl-Sys-Syslog perl-LWP-Protocol-https
perl-Digest-SHA --enablerepo="rhui-REGION-rhel-server-optional" -y
sudo yum install zip unzip
```

Para instalar os pacotes necessários no Red Hat Enterprise Linux 6.9

1. Iniciar a sessão na sua instância. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. Em um prompt de comando, instale pacotes da forma a seguir:

```
sudo yum install perl-Datetime perl-CPAN perl-Net-SSLeay perl-IO-Socket-SSL perl-
Digest-SHA gcc -y
sudo yum install zip unzip
```

3. Execute o CPAN como um usuário elevado:

```
sudo cpan
```

Pressione ENTER nas solicitações até ver a seguinte solicitação:

```
cpan[1]>
```

4. Na solicitação do CPAN, execute cada um dos comandos abaixo: execute um comando e ele será instalado. Depois, retorne à solicitação do CPAN e execute o próximo comando. Pressione ENTER como antes quando solicitado para continuar o processo:

```
cpan[1]> install YAML
cpan[2]> install LWP::Protocol::https
cpan[3]> install Sys::Syslog
cpan[4]> install Switch
```

Para instalar os pacotes necessários no SUSE

1. Iniciar a sessão na sua instância. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. Nos servidores que executam o SUSE Linux Enterprise Server 12, talvez seja necessário fazer download do pacote perl-Switch. É possível fazer download e instalar esse pacote com os seguintes comandos:

```
wget http://download.opensuse.org/repositories/devel:/languages:/perl/SLE_12_SP3/
noarch/perl-Switch-2.17-32.1.noarch.rpm
```

```
sudo rpm -i perl-Switch-2.17-32.1.noarch.rpm
```

3. Instale os pacotes necessários da seguinte maneira:

```
sudo zypper install perl-Switch perl-Datetime  
sudo zypper install -y "perl(LWP::Protocol::https)"
```

## Instalar scripts de monitoramento

A etapas a seguir mostram como fazer download, descompactar e configurar os scripts de monitoramento do CloudWatch em uma instância do EC2 Linux.

Para fazer download, instalar e configurar os scripts de monitoramento

1. Em um prompt de comando, mova para uma pasta onde você deseja armazenar os scripts de monitoramento e execute o comando a seguir para fazer download deles:

```
curl https://aws-cloudwatch.s3.amazonaws.com/downloads/  
CloudWatchMonitoringScripts-1.2.2.zip -O
```

2. Execute os comandos a seguir para instalar os scripts de monitoramento que você fez download:

```
unzip CloudWatchMonitoringScripts-1.2.2.zip && \  
rm CloudWatchMonitoringScripts-1.2.2.zip && \  
cd aws-scripts-mon
```

O pacote para os scripts de monitoramento contém os arquivos a seguir:

- CloudWatchClient.pm: módulo Perl compartilhado que simplifica o acesso ao Amazon CloudWatch de outros scripts.
- mon-put-instance-data.pl: coleta as métricas do sistema em uma instância do Amazon EC2 (memória, swap, utilização do espaço em disco) e os envia para o Amazon CloudWatch.
- mon-get-instance-stats.pl: consulta o Amazon CloudWatch e exibe a estatística de utilização mais recente para a instância do EC2 na qual este script é executado.
- awscreds.template: modelo de arquivo para credenciais da AWS que armazena o ID da chave de acesso e a chave de acesso secreta.
- LICENSE.txt: arquivo de texto que contém a licença do Apache 2.0.
- NOTICE.txt: aviso de direitos autorais.

## mon-put-instance-data.pl

Esse script coleta dados de memória, swap uso de espaço em disco no sistema atual. Isso, então, faz uma chamada remota para o Amazon CloudWatch relatar os dados coletados como métricas personalizadas.

### Options

Nome	Descrição
--mem-util	Coleta e envia as métricas de MemoryUtilization nas porcentagens. Essa métrica conta a memória alocada por aplicativos e pelo sistema operacional conforme usada, além de incluir cache e memória de buffer conforme usado caso você especifique a opção --mem-used-incl-cache-buff.

Nome	Descrição
--mem-used	Coleta e envia as métricas de MemoryUsed, relatadas em megabytes. Essa métrica conta a memória alocada por aplicativos e pelo sistema operacional conforme usada, além de incluir cache e memória de buffer conforme usado caso você especifique a opção --mem-used-incl-cache-buff.
--mem-used-incl-cache-buff	Se você incluir essa opção, a memória usada atualmente no cache e nos buffers será contada como "usada" quando as métricas são relatadas para --mem-util, --mem-used e --mem-avail.
--mem-avail	Coleta e envia as métricas de MemoryAvailable, relatadas em megabytes. Essa métrica conta a memória alocada por aplicativos e pelo sistema operacional conforme usada, além de incluir cache e memória de buffer conforme usado caso você especifique a opção --mem-used-incl-cache-buff.
--swap-util	Recolhe e envia as métricas de SwapUtilization, relatadas em porcentagens.
--swap-used	Coleta e envia as métricas de SwapUsed, relatadas em megabytes.
--disk-path=PATH	Seleciona o disco no qual fazer o relatório.  CAMINHO pode especificar um ponto de montagem ou qualquer arquivo localizado em um ponto de montagem para o filesystem que precisa ser relatado. Para selecionar múltiplos discos, especifique um --disk-path=PATH para cada um deles.  Para selecionar um disco para os filesystems montados em / e /home, use os parâmetros a seguir:  --disk-path=/ --disk-path=/home
--disk-space-util	Coleta e envia a métrica de DiskSpaceUtilization para os discos selecionados. A métrica é relatada em porcentagens.  Observe que as métricas de utilização de disco calculadas por esse script diferem dos valores calculados pelo comando df -k -l. Se você achar os valores de df -k -l mais úteis, pode alterar os cálculos no script.
--disk-space-used	Coleta e envia a métrica DiskSpaceUsed para os discos selecionados. A métrica é relatada por padrão em gigabytes.  Devido a um espaço em disco reservado nos sistemas operacionais Linux, espaço em disco usado e espaço em disco disponível podem não totalizar com precisão no total de espaço em disco.
--disk-space-avail	Coleta e envia a métrica DiskSpaceAvailable para os discos selecionados. A métrica é relatada em gigabytes.  Devido a um espaço em disco reservado nos sistemas operacionais Linux, espaço em disco usado e espaço em disco disponível podem não totalizar com precisão no total de espaço em disco.

Nome	Descrição
--memory-units=UNITS	Especifica as unidades nas quais deve ser relatado o uso da memória. Se não tiver especificado, a memória é relatada em megabytes. UNIDADES pode ser uma das seguintes opções: bytes, kilobytes, megabytes, gigabytes.
--disk-space-units=UNITS	Especifica as unidades nas quais deve ser relatado o uso do espaço em disco. Se não estiver especificado, o espaço em disco é relatado em gigabytes. UNIDADES pode ser uma das seguintes opções: bytes, kilobytes, megabytes, gigabytes.
--aws-credential-file=PATH	Fornece a localização do arquivo que contém as credenciais da AWS.  Esse parâmetro não pode ser usado com os parâmetros --aws-access-key-id e --aws-secret-key.
--aws-access-key-id=VALUE	Especifica o ID da chave de acesso da AWS a ser usado para identificar o autor da chamada. Deve ser usado em conjunto com a opção --aws-secret-key. Não use esta opção com o parâmetro --aws-credential-file.
--aws-secret-key=VALUE	Especifica a chave de acesso secreta da AWS a ser usada para assinar a solicitação para o CloudWatch. Deve ser usado em conjunto com a opção --aws-access-key-id. Não use esta opção com o parâmetro --aws-credential-file.
--aws-iam-role=VALUE	Especifica a função do IAM usada para fornecer credenciais da AWS. O valor =VALUE é obrigatório. Se nenhuma credencial for especificada, a função do IAM padrão associado com a instância do EC2 é aplicada. Apenas uma função do IAM pode ser usado. Se nenhuma função do IAM for encontrada, ou se mais de uma função do IAM for encontrada, o script apresentará um erro.  Não use esta opção com os parâmetros --aws-credential-file, --aws-access-key-id ou --aws-secret-key.
--aggregated[=only]	Adiciona métricas agregadas para o tipo de instância, ID da AMI e geral para a região. O valor =only é opcional; se especificado, o script relata somente métricas agregadas.
--auto-scaling[=only]	Adiciona métricas agregadas para o grupo de Auto Scaling. O valor =only é opcional; se especificado, o script relata somente métricas de Auto Scaling. A <a href="#">política do IAM</a> associada à conta ou função do IAM que usa os scripts necessários para ter permissão para chamar a ação do EC2 <a href="#">DescribeTags</a> .
--verify	Executa uma execução de teste do script que coleta as métricas, prepara uma solicitação HTTP concluída, mas não acessa de fato o CloudWatch para relatar os dados. Essa opção também verifica se foram fornecidas credenciais. Quando executada no modo detalhado, essa opção resulta em métricas que serão enviadas ao CloudWatch.
--from-cron	Use esta opção para chamar o script de cron. Quando essa opção for usada, todas as saídas diagnósticas são suprimidas, mas mensagens de erro são enviadas ao log do sistema local da conta de usuário.

Nome	Descrição
--verbose	Exibe informações detalhadas sobre o que o script está fazendo.
--help	Exibe informações de uso.
--version	Exibe o número de versão do script.

### Examples

Os exemplos a seguir pressupõem que você forneceu uma função do IAM ou arquivo `awscreds.conf`. Caso contrário, você deve fornecer as credenciais que usam os parâmetros `--aws-access-key-id` e `--aws-secret-key` para esses comandos.

O exemplo a seguir realiza uma execução de teste simples sem publicar dados no CloudWatch.

```
./mon-put-instance-data.pl --mem-util --verify --verbose
```

O exemplo a seguir coleta todas as métricas de memória disponíveis e as envia ao CloudWatch, contando a memória em cache e buffer como usada

```
./mon-put-instance-data.pl --mem-used-incl-cache-buff --mem-util --mem-used --mem-avail
```

O exemplo a seguir coleta métricas agregadas para um grupo de Auto Scaling e as envia ao Amazon CloudWatch sem relatar métricas de instância individuais.

```
./mon-put-instance-data.pl --mem-util --mem-used --mem-avail --auto-scaling=only
```

O exemplo a seguir coleta métricas agregadas para o tipo de instância, o ID da AMI e a região, e as envia ao Amazon CloudWatch sem relatar métricas de instância individuais

```
./mon-put-instance-data.pl --mem-util --mem-used --mem-avail --aggregated=only
```

Para definir uma programação cron para métricas relatadas ao CloudWatch, inicie editando o crontab usando o comando `crontab -e`. Adicione o comando a seguir para relatar utilização de memória e espaço em disco para o CloudWatch a cada cinco minutos:

```
*/5 * * * * ~/aws-scripts-mon/mon-put-instance-data.pl --mem-used-incl-cache-buff --mem-util --disk-space-util --disk-path=/ --from-cron
```

Se o script encontrar um erro, ele gravará a mensagem de erro no log do sistema.

## mon-get-instance-stats.pl

Este script consulta CloudWatch para estatísticas de métricas de memória, swap e espaço em disco dentro do intervalo de tempo usando o número de horas mais recentes. Esses dados são fornecidos para a instância do Amazon EC2 na qual o script é executado.

### Options

Nome	Descrição
<code>--recent-hours=N</code>	Especifica o número de horas recentes para relatar, como representado por <code>N</code> , onde <code>N</code> é um inteiro.

Nome	Descrição
--aws-credential-file=PATH	Fornece a localização do arquivo que contém as credenciais da AWS.
--aws-access-key-id=VALUE	Especifica o ID da chave de acesso da AWS a ser usado para identificar o autor da chamada. Deve ser usado em conjunto com a opção --aws-secret-key. Não use esta opção com a opção --aws-credential-file.
--aws-secret-key=VALUE	Especifica a chave de acesso secreta da AWS a ser usada para assinar a solicitação para o CloudWatch. Deve ser usado em conjunto com a opção --aws-access-key-id. Não use esta opção com a opção --aws-credential-file.
--aws-iam-role=VALUE	Especifica a função do IAM usada para fornecer credenciais da AWS. O valor =VALUE é obrigatório. Se nenhuma credencial for especificada, a função do IAM padrão associado com a instância do EC2 é aplicada. Apenas uma função do IAM pode ser usado. Se nenhuma função do IAM for encontrada, ou se mais de uma função do IAM for encontrada, o script apresentará um erro.  Não use esta opção com os parâmetros --aws-credential-file, --aws-access-key-id ou --aws-secret-key.
--verify	Realiza uma execução de teste do script. Essa opção também verifica se foram fornecidas credenciais.
--verbose	Exibe informações detalhadas sobre o que o script está fazendo.
--help	Exibe informações de uso.
--version	Exibe o número de versão do script.

#### Example

Para obter estatísticas de utilização pelas últimas 12 horas, execute o comando a seguir:

```
./mon-get-instance-stats.pl --recent-hours=12
```

Esta é uma resposta de exemplo:

```
Instance metric statistics for the last 12 hours.

CPU Utilization
    Average: 1.06%, Minimum: 0.00%, Maximum: 15.22%

Memory Utilization
    Average: 6.84%, Minimum: 6.82%, Maximum: 6.89%

Swap Utilization
    Average: N/A, Minimum: N/A, Maximum: N/A

Disk Space Utilization on /dev/xvda1 mounted as /
    Average: 9.69%, Minimum: 9.69%, Maximum: 9.69%
```

## Visualizar as métricas personalizadas no console

Após executar com êxito o script `mon-put-instance-data.pl`, você pode visualizar as métricas personalizadas no console Amazon CloudWatch.

Para exibir métricas personalizadas

1. Execute `mon-put-instance-data.pl` conforme descrito previamente.
2. Abra o console do CloudWatch em <https://console.aws.amazon.com/cloudwatch/>.
3. Selecione Exibir métricas.
4. Para Visualização, suas métricas personalizadas publicadas pelo script são exibidas com o prefixo `System/Linux`.

## Troubleshoot

O módulo CloudWatchClient.pm coloca em cache metadados da instância localmente. Se você criar uma AMI por uma instância na qual executa os scripts de monitoramento, quaisquer instâncias executadas pelas AMIs de dentro do TTL do cache (padrão: 6 horas, 24 horas para os grupos do Auto Scaling) emitiriam métricas usando o ID da instância da instância original. Após o período de TTL em cache passar, o script recuperará dados frescos e os scripts de monitoramento usarão o ID da instância atual. Para corrigir disso imediatamente, remova os dados armazenados em cache usando o comando a seguir:

```
rm /var/tmp/aws-mon/instance-id
```

## 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 AWS. 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",  
            "detailType": "AWS API Call via CloudTrail",  
            "requestParameters": {  
                "Action": "TerminateInstances",  
                "DryRun": "false",  
                "MaxAttempts": 1,  
                "MinAttempts": 1,  
                "TerminationType": "Graceful",  
                "InstanceIds": ["i-000000000000000000"],  
                "Region": "us-west-2"  
            },  
            "responseElements": {},  
            "awsRegion": "us-west-2",  
            "cloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-group:/aws/ec2/2016/05/20/08/27/45/  
            "cloudWatchLogsLogStreamArn": "arn:aws:logs:us-west-2:123456789012:log-stream:/aws/ec2/2016/05/20/08/27/45/  
        }  
    ]  
}
```

```
"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": "ABCDEFGNOMOOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/ec2-instance-connect"
    },
    "version": "1.05"
}
```

```
"arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
"accountId": "123456789012",
"accessKeyId": "ABCDEFGUZHNAW4OSN2AEXAMPLE",
"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).

# 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 \(p. 923\)](#)
- [Endereçamento IP de instâncias do Amazon EC2 \(p. 937\)](#)
- [Traga seus próprios endereços IP \(BYOIP\) no Amazon EC2 \(p. 954\)](#)
- [Atribuição de prefixos a interfaces de rede do Amazon EC2 \(p. 963\)](#)
- [Endereços IP elásticos \(p. 975\)](#)
- [Interfaces de rede elástica \(p. 984\)](#)
- [Largura de banda de rede de instâncias do Amazon EC2 \(p. 1013\)](#)
- [Rede avançada no Linux \(p. 1015\)](#)
- [Elastic Fabric Adapter \(p. 1044\)](#)
- [Grupos de posicionamento \(p. 1084\)](#)
- [Unidade de transmissão máxima \(MTU\) de rede para a instância do EC2 \(p. 1096\)](#)
- [Nuvens privadas virtuais \(p. 1100\)](#)
- [EC2-Classic \(p. 1100\)](#)

# 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 \(p. 924\)](#)
- [Zonas de disponibilidade \(p. 928\)](#)
- [Local Zones \(p. 930\)](#)
- [Zonas do Wavelength \(p. 934\)](#)
- [AWS Outposts \(p. 936\)](#)

## 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 \(p. 144\)](#).

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 \(p. 924\)](#)
- [Regiões e endpoints \(p. 926\)](#)
- [Descreva suas regiões \(p. 926\)](#)
- [Obter o nome da região \(p. 927\)](#)
- [Especificar a região para um recurso \(p. 927\)](#)

## 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” \(p. 931\)](#).

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 \(p. 926\)](#).

## 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.

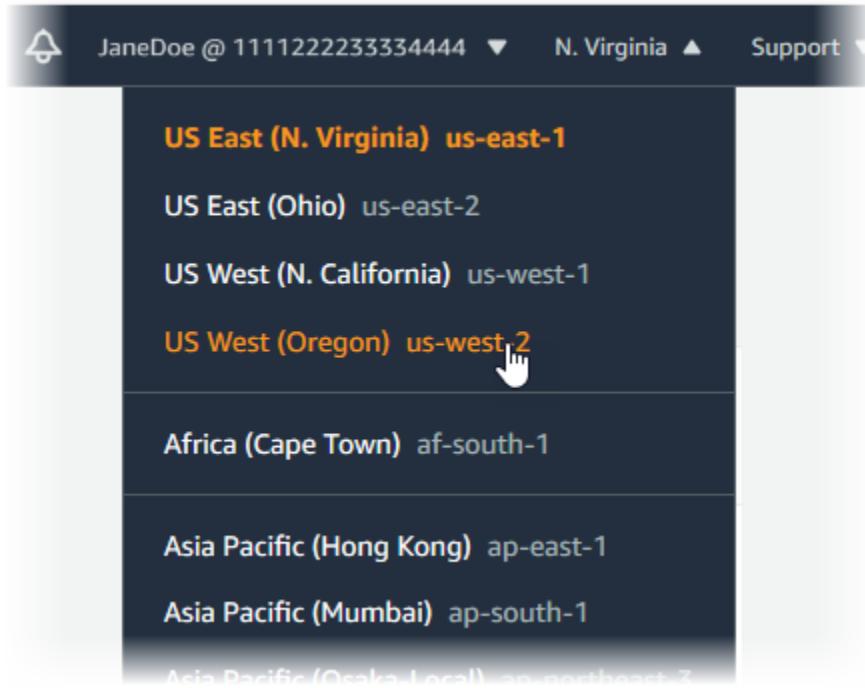
Para obter mais informações sobre os endpoints e os protocolos em AWS GovCloud (Oeste dos EUA), consulte [AWS GovCloud \(US-West\) Endpoints](#) (Endpoints da AWS GovCloud (Oeste dos EUA)) no AWS GovCloud (US) User Guide (Manual do usuário da AWS GovCloud (EUA)).

## 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)

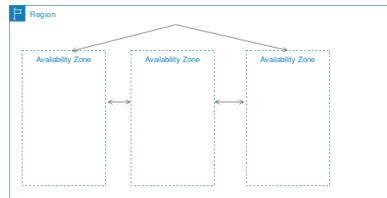
Como alternativa, você pode usar o código `--region` (AWS CLI) ou a opção da linha de comando `-Region` (AWS Tools for Windows PowerShell) com cada comando individual. Por exemplo, `--region us-east-2`.

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 \(p. 975\)](#).

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 \(p. 929\)](#)
- [Executar instâncias em uma zona de disponibilidade \(p. 929\)](#)
- [Migrar uma instância para outra zona de disponibilidade \(p. 930\)](#)

## 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:

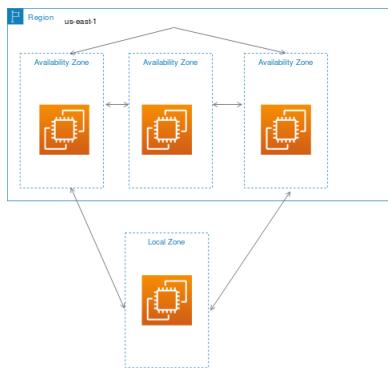
- Criação de uma AMI da instância original
- Execução de uma instância na nova zona de disponibilidade
- Atualização da configuração da nova instância, conforme mostrado no procedimento a seguir

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 \(p. 929\)](#).
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 \(p. 980\)](#).
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 \(p. 380\)](#).
6. (Opcional) Encerre a instância original. Para obter mais informações, consulte [Como encerrar uma instância \(p. 589\)](#).

## 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-lax-1a`. Para obter mais informações, consulte [Local Zones disponíveis \(p. 931\)](#).

Para usar uma Local Zone, é necessário ativá-la primeiro. Para obter mais informações, consulte [the section called “Optar por Local Zones” \(p. 933\)](#). 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 \(p. 931\)](#)
- [Descreva suas Local Zones \(p. 932\)](#)
- [Optar por Local Zones \(p. 933\)](#)
- [Executar instâncias em uma Local Zone \(p. 933\)](#)

## 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” \(p. 933\)](#).

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:

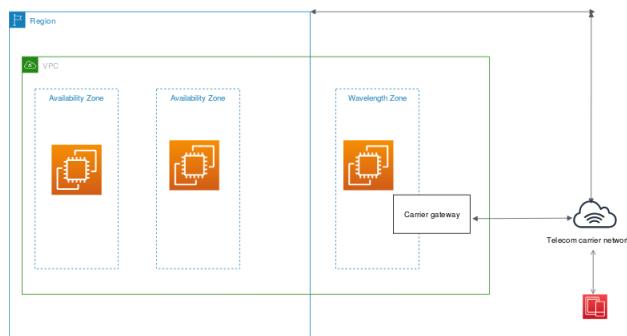
1. Habilite as Local Zones. Para obter mais informações, consulte [Optar por Local Zones \(p. 933\)](#).

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 \(p. 509\)](#).

## 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” \(p. 935\)](#). 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 \(p. 934\)](#)
- [Habilitar zonas de Wavelength \(p. 935\)](#)
- [Executar instâncias em uma zona de Wavelength \(p. 936\)](#)

## 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 \(p. 1438\)](#).

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 \(p. 1407\)](#).

## 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 \(p. 937\)](#)
- [Endereços IPv4 públicos e nomes de host DNS externos \(p. 938\)](#)
- [Endereços IP elásticos \(IPv4\) \(p. 939\)](#)
- [Servidor DNS da Amazon \(p. 939\)](#)
- [Endereços IPv6 \(p. 939\)](#)
- [Trabalhar com os endereços IPv4 para as instâncias \(p. 940\)](#)
- [Trabalhar com os endereços IPv6 para as instâncias \(p. 943\)](#)
- [Vários endereços IP \(p. 946\)](#)

## 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 \(p. 946\)](#).

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 \(p. 942\)](#).

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 \(p. 975\)](#).

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 \(p. 975\)](#).

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 \(p. 986\)](#).

## 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 \(p. 940\)](#)
- [Atribuir um endereço IPv4 público durante a execução da instância \(p. 942\)](#)

## 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 \(p. 649\)](#).

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 [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. Use o comando a seguir para acessar o endereço IP privado:

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/local-ipv4
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4
```

3. Use o comando a seguir para acessar o endereço IP público:

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/public-ipv4
```

IMDSv1

```
[ec2-user ~]$ curl 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 \(p. 938\)](#). 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 \(p. 975\)](#).

- Você não 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 \(p. 975\)](#). 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. \(p. 510\)](#). 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 \(p. 944\)](#)
- [Atribuir um endereço IPv6 a uma instância \(p. 945\)](#)
- [Cancelar a atribuição de um endereço IPv6 de uma instância \(p. 945\)](#)

## 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 (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 (IPv6).
5. Como alternativa, em Network interfaces (Interfaces de rede) na guia Description (Descrição), escolha eni-eth0 e depois escolha o ID da interface (por exemplo, eni-123abc456def78901). Localize IPv6 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 [Conecte-se à sua instância do Linux \(p. 535\)](#).
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/>).

### 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/network/interfaces/macs/mac-address/ipv6s
```

IMDSv1

```
[ec2-user ~]$ curl 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 \(p. 986\)](#).

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 \(p. 946\)](#)
- [Trabalhar com vários endereços IPv4 \(p. 947\)](#)
- [Trabalhar com vários endereços IPv6 \(p. 951\)](#)

## 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 \(p. 947\)](#)
- [Configurar o sistema operacional na instância para reconhecer endereços IPv4 privados secundários \(p. 949\)](#)
- [Associar um endereço IP elástico ao endereço IPv4 privado secundário \(p. 949\)](#)
- [Visualizar endereços IPv4 privados secundários \(p. 950\)](#)
- [Cancelar a atribuição de um endereço IPv4 privado secundário \(p. 950\)](#)

### 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 \(p. 948\)](#)
- [Para atribuir um endereço IPv4 secundário durante a execução usando a linha de comando \(p. 948\)](#)
- [Para atribuir um endereço IPv4 privado secundário a uma interface de rede \(p. 948\)](#)
- [Para atribuir um IPv4 privado secundário a uma instância existente usando a linha de comando \(p. 949\)](#)

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 \(p. 986\)](#).

**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 \(p. 976\)](#).

- 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 \(p. 949\)](#).

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.

- Se estiver usando o Amazon Linux, o pacote ec2-net-utils poderá cuidar desta etapa para você. Ele configura interfaces de rede adicionais que você anexa enquanto a instância está em execução, atualiza os endereços IPv4 secundários durante a renovação da concessão DHCP e atualiza a regras de roteamento relacionadas. Você pode atualizar a lista de interfaces imediatamente usando o comando `sudo service network restart` e, em seguida, visualizar a lista atualizada usando `ip addr`. Se você precisar de controle manual sobre a configuração da rede, poderá remover o pacote ec2-net-utils. Para obter mais informações, consulte [Configurar a interface de rede usando ec2-net-utils \(p. 1011\)](#).
- Se estiver usando outra distribuição do Linux, consulte a documentação da distribuição do Linux. Procure informações sobre como configurar interfaces de rede adicionais e endereços IPv4 secundários. Se a instância tiver duas ou mais interfaces na mesma sub-rede, pesquise as informações sobre como usar as regras de roteamento para resolver roteamento assimétrico.

Para obter informações sobre como configurar uma instância Windows, consulte [Como configurar um endereço IP privado secundário para a instância Windows em uma VPC](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## 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 \(p. 951\)](#)
- [Visualizar os endereços IPv6 \(p. 953\)](#)
- [Cancelar a atribuição de um endereço IPv6 \(p. 953\)](#)

## 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 \(p. 203\)](#).
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 \(p. 986\)](#).

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 \(p. 1240\)](#). 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 \(p. 954\)](#)
- [Configurar seu intervalo de endereços BYOIP \(p. 955\)](#)
- [Trabalhar com o intervalo de endereços \(p. 962\)](#)
- [Saiba mais \(p. 963\)](#)

## 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 \(p. 960\)](#).
- 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 \(p. 955\)](#)
- [Criar um objeto ROA em seu RIR \(p. 959\)](#)
- [Atualizar o registro RDAP em seu RIR \(p. 959\)](#)
- [Provisionar o intervalo de endereços em AWS \(p. 959\)](#)
- [Anunciar o intervalo de endereços por meio da AWS \(p. 961\)](#)
- [Desprovisionar o intervalo de endereços \(p. 961\)](#)

## 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-----
MIIEVgIBADANBgkqhkiG9w0BAQEFAASCBGwgGSKAgEAAoIBAQDFBXRI4HVKAhh
3seiciooiCzRTbJe1+YsxNTja4XyKpVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv510tJKk+a91K4+t03UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRs01AhJ
DnZPNeweboo+K3Q3lwgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzSPVuDLAgMBAAECggEACiJuJ2hfJkV47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKnbshoJGuFfwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNr1h0jDhpicL8cQEbdBjyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULmlWiAZ3MRAZPjHHgpVkyAAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQbGqdjwlC/3jxp8zJy6P8o
JQKV7TdvMuuj4VSWOHZBHLv4evJaia1ouQjIo1UDA8AYitqhX1NmCehGH8yuXj/
v6V3CzMKDkmRr1NrONNsZ5QsndQ04Z6ihAq1PmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85g0e1i8kwZws+xlpG6uBT6lmIJEld0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWBxXiyyT0o8szjnJ1En8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqvHOGMxj7quhneBq2T6FbiLD
T9TV1YaGNZ0j71vQaL119qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjd
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW91Itu8aBrMndnQKBgQDb
nNp/JyRwjqOrN1jk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yu1QcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTxqhXDdrsswWIvYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZxWdIhYyI3QKBgD+F/6wcZ85QW8naUyka
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxkdn8QV0b5p3WuWH1U8B
-----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:d5:95:86:35:  
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:c9: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-----  
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAx0Vx0SOB1SgIYd7HonIq  
KISwkU2yXtfmLMTU42uF8isqVRiBVgx0WbOOBQh5Tzjk1Sfjaj++MPeqD0wz0t8a  
PZGkMmQRZ9mBKdhAAub399OyhzUzmWVJpJ9MxzkhKTZmNnzMSEgcXsJcURQJ4sJk  
nf/Ew7xyTGPRbwCL1rk7L+ZdLSSpPmvdsuPrTt1H0e0p6OV1xMX7Aa1t4NcnaN0  
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](mailto: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 confirmado que é o proprietário do intervalo de endereços e autoriza a Amazon a anunciar o. 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-byoip-cidrs](#) para monitorar seu progresso, como neste exemplo:

```
aws ec2 describe-byoip-cidrs --max-results 5
```

Se houver problemas durante o provisionamento e o status for para `failed-provision`, o comando [provision-byoip-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-byoip-cidr](#).

```
aws ec2 provision-byoip-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 anunciarlo 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 \(p. 976\)](#).

#### Limitations

- Você pode executar o comando `advertise-byoip-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-12345678abcaabcabc
```

(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 online [Mergulho 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 \(p. 964\)](#)

- [Considerações e limites para prefixos \(p. 964\)](#)
- [Trabalhar com prefixos \(p. 964\)](#)

## 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-1` Região 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 \(p. 986\)](#).
- 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 `umc5.1large` instância, 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 \(p. 965\)](#)
- [Atribuir prefixos a interfaces de rede existentes \(p. 969\)](#)
- [Configure seu sistema operacional para interfaces de rede com prefixos \(p. 972\)](#)
- [Exibir os prefixos atribuídos às suas interfaces de rede \(p. 972\)](#)

- [Remover prefixos de suas interfaces de rede \(p. 974\)](#)

## 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 \(p. 972\)](#).

### Tópicos

- [Atribuir prefixos automáticos durante a criação da interface de rede \(p. 965\)](#)
- [Atribuir prefixos específicos durante a criação da interface de rede \(p. 967\)](#)

## 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 `--ipv4-prefix-count` para o número de prefixos que você deseja AWS atribuir. No exemplo a seguir, o AWS atribui 1 prefixo.

```
$ 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 `aws ec2 create-network-interface` comando e setar o `--ipv6-prefix-count` para o número de prefixos que você deseja atribuir. No exemplo a seguir, o AWS atribuiu 1 prefixo.

```
$ 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": [  
            {  
                "Primary": true,  
                "PrivateIpAddress": "10.0.0.62",  
                "Ipv6Address": "2606:4700::62/  
            }  
        ],  
        "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"  
    }  
}
```

```
{  
    "GroupName": "default",  
    "GroupId": "sg-044c2de2c4EXAMPLE"  
}  
,  
"InterfaceType": "interface",  
"Ipv6Addresses": [],  
"MacAddress": "02:bb:e4:31:fe:09",  
"NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",  
"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 `acreate-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.

```
$ 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 `acreate-network-interface` Comando e set--ipv6-prefixes para os prefixos. AWS seleciona endereços IP deste intervalo. No exemplo a seguir, o prefixo CIDR é 2600:1f13:fc2:a700:1768::/80.

```
$ 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-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": "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 \(p. 972\)](#).

### 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 desejaAWSatribuir. No exemplo a seguir, oAWSatribui1Prefixo IPv4.

```
$ 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 [aassign-ipv6-addresses](#)Comando e set--[ipv6-prefix-count](#)para o número de prefixos que você desejaAWSatribuir. No exemplo a seguir, oAWSatribui1Prefixo IPv6.

```
$ 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

Deleção 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 `aassign-private-ip-addresses` Comando e set--ipv4-prefixes Para o prefixo. AWS seleciona endereços IPv4 deste intervalo. No exemplo a seguir, o prefixo CIDR é 10.0.0.208/28.

```
$ 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 `aassign-ipv6-addresses` Comando e set--ipv6-prefixes Para o prefixo. AWS seleciona endereços IPv6 deste intervalo. No exemplo a seguir, o prefixo CIDR é 2600:1f13:fc2:a700:18bb::/80.

```
$ aws ec2 assign-ipv6-addresses \  
--network-interface-id eni-081fbb4095EXAMPLE \  
--ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

```
--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 `describe-network-interfaces` AWS CLI para exibir os prefixos atribuídos às interfaces de rede.

```
$ 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-006edbcfa4EXAMPLE",
    "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 o `unassign-private-ip-addresses` Comando e set `--ipv4-prefix` Para o endereço que você deseja remover.

```
$ 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 `unassign-ipv6-addresses` Comando e set `--ipv6-prefix` Para o endereço que você deseja remover.

```
$ 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 do , ou [Configurar um DNS dinâmico na instância do Amazon Linux \(p. 640\)](#).

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 \(p. 975\)](#)
- [Noções básicas sobre endereços IP elásticos \(p. 975\)](#)
- [Trabalhar com endereços IP elásticos \(p. 976\)](#)
- [Usar DNS reverso para aplicações de e-mail \(p. 982\)](#)
- [Limite de endereços IP elásticos \(p. 983\)](#)

## 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 \(p. 938\)](#).
- 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 \(p. 983\)](#).
- 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 \(p. 976\)](#)
- [Descrever seus endereços IP elásticos \(p. 977\)](#)
- [Aplicar uma tag em um endereço IP elástico \(p. 978\)](#)
- [Associar um endereço IP elástico a uma instância ou interface de rede \(p. 979\)](#)
- [Dissociar um endereço IP elástico \(p. 980\)](#)
- [Liberar um endereço IP elástico \(p. 981\)](#)
- [Recuperar um endereço IP elástico \(p. 982\)](#)

## 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 \(p. 954\)](#).

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 \(p. 1012\)](#).

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 \(p. 984\)](#)
- [Placas de rede \(p. 986\)](#)
- [Endereços IP por interface de rede por tipo de instância \(p. 986\)](#)
- [Trabalhar com interfaces de rede \(p. 1001\)](#)
- [Cenários para interfaces de rede \(p. 1009\)](#)
- [Melhores práticas para configurar interfaces de rede \(p. 1011\)](#)
- [Interfaces de rede gerenciadas pelo solicitante \(p. 1012\)](#)

## 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 \(p. 986\)](#).

#### 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 \(p. 938\)](#).

#### 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 \(p. 939\)](#).

#### 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.

## Placas de rede

As instâncias com várias placas de rede oferecem maior performance de rede, incluindo recursos de largura de banda acima de 100 Gbps e maior performance da taxa de pacotes. Cada interface de rede é conectada a uma placa de rede. A interface de rede primária deve ser atribuída ao índice 0 da placa de rede.

Se você ativar Elastic Fabric Adapter (EFA) ao executar uma instância compatível com várias placas de rede, todas as placas de rede estarão disponíveis. Você pode atribuir até uma EFA por placa de rede. Uma EFA conta como uma interface de rede.

As instâncias a seguir suportam várias placas de rede. Todos os outros tipos de instância suportam uma placa de rede.

Tipo de instância	Quantidade de placas de rede
p4d.24xlarge	4

## 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
a1.medium	2	4	4
a1.large	3	10	10
a1.xlarge	4	15	15
a1.2xlarge	4	15	15
a1.4xlarge	8	30	30
a1.metal	8	30	30
c1.medium	2	6	IPv6 não compatível
c1.xlarge	4	15	IPv6 não compatível
c3.large	3	10	10

Amazon Elastic Compute Cloud Manual  
 do usuário para instâncias do Linux  
 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
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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
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
c5n.9xlarge	8	30	30
c5n.18xlarge	15	50	50
c5n.metal	15	50	50
c6g.medium	2	4	4
c6g.large	3	10	10
c6g.xlarge	4	15	15
c6g.2xlarge	4	15	15
c6g.4xlarge	8	30	30
c6g.8xlarge	8	30	30
c6g.12xlarge	8	30	30
c6g.16xlarge	15	50	50
c6g.metal	15	50	50
c6gd.medium	2	4	4

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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
c6gd.large	3	10	10
c6gd.xlarge	4	15	15
c6gd.2xlarge	4	15	15
c6gd.4xlarge	8	30	30
c6gd.8xlarge	8	30	30
c6gd.12xlarge	8	30	30
c6gd.16xlarge	15	50	50
c6gd.metal	15	50	50
c6gn.medium	2	4	4
c6gn.large	3	10	10
c6gn.xlarge	4	15	15
c6gn.2xlarge	4	15	15
c6gn.4xlarge	8	30	30
c6gn.8xlarge	8	30	30
c6gn.12xlarge	8	30	30
c6gn.16xlarge	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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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
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
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
inf1.xlarge	4	10	10
inf1.2xlarge	4	10	10
inf1.6xlarge	8	30	30
inf1.24xlarge	15	30	30
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

Amazon Elastic Compute Cloud Manual  
 do usuário para instâncias do Linux  
 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
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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
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
m6g.medium	2	4	4
m6g.large	3	10	10
m6g.xlarge	4	15	15
m6g.2xlarge	4	15	15
m6g.4xlarge	8	30	30
m6g.8xlarge	8	30	30
m6g.12xlarge	8	30	30
m6g.16xlarge	15	50	50
m6g.metal	15	50	50
m6gd.medium	2	4	4
m6gd.large	3	10	10
m6gd.xlarge	4	15	15
m6gd.2xlarge	4	15	15
m6gd.4xlarge	8	30	30
m6gd.8xlarge	8	30	30
m6gd.12xlarge	8	30	30
m6gd.16xlarge	15	50	50
m6gd.metal	15	50	50
m6i.large	3	10	10
m6i.xlarge	4	15	15
m6i.2xlarge	4	15	15
m6i.4xlarge	8	30	30

Amazon Elastic Compute Cloud Manual  
 do usuário para instâncias do Linux  
 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
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
mac1.metal	8	30	30
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
p4d.24xlarge	4x15	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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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
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
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
r6g.medium	2	4	4
r6g.large	3	10	10
r6g.xlarge	4	15	15
r6g.2xlarge	4	15	15

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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
r6g.4xlarge	8	30	30
r6g.8xlarge	8	30	30
r6g.12xlarge	8	30	30
r6g.16xlarge	15	50	50
r6g.metal	15	50	50
r6gd.medium	2	4	4
r6gd.large	3	10	10
r6gd.xlarge	4	15	15
r6gd.2xlarge	4	15	15
r6gd.4xlarge	8	30	30
r6gd.8xlarge	8	30	30
r6gd.12xlarge	8	30	30
r6gd.16xlarge	15	50	50
r6gd.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
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

Amazon Elastic Compute Cloud Manual  
 do usuário para instâncias do Linux  
 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
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
t4g.nano	2	2	2
t4g.micro	2	2	2
t4g.small	3	4	4
t4g.medium	3	6	6
t4g.large	3	12	12
t4g.xlarge	4	15	15
t4g.2xlarge	4	15	15
u-6tb1.56xlarge	15	50	50
u-6tb1.112xlarge	15	50	50
u-6tb1.metal	15	50	50
u-9tb1.112xlarge	15	50	50
u-9tb1.metal	15	50	50
u-12tb1.112xlarge	15	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

Tipo de instância	Máximo de interfaces de rede	Endereços IPv4 privados por interface	Endereços IPv6 por interface
x2gd.medium	2	4	4
x2gd.large	3	10	10
x2gd.xlarge	4	15	15
x2gd.2xlarge	4	15	15
x2gd.4xlarge	8	30	30
x2gd.8xlarge	8	30	30
x2gd.12xlarge	8	30	30
x2gd.16xlarge	15	50	50
x2gd.metal	15	50	50
z1d.large	3	10	10
z1d.xlarge	4	15	15
z1d.2xlarge	4	15	15
z1d.3xlarge	8	30	30
z1d.6xlarge	8	30	30
z1d.12xlarge	15	50	50
z1d.metal	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 \(p. 1001\)](#)
- [Visualizar detalhes sobre uma interface de rede \(p. 1002\)](#)
- [Anexar uma interface de rede a uma instância. \(p. 1003\)](#)
- [Desanexar uma interface de rede de uma instância \(p. 1004\)](#)
- [Gerenciar endereços IP \(p. 1005\)](#)
- [Modificar atributos da interface de rede \(p. 1006\)](#)
- [Adicionar ou editar tags \(p. 1007\)](#)
- [Excluir uma interface de rede \(p. 1008\)](#)

## 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 descriptivo.
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](#) ou [Network Interfaces](#) de rede Página do console do Amazon EC2. Se preferir, você pode associar uma interface de rede existente ao [iniciar instâncias \(p. 510\)](#).

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 \(p. 938\)](#).

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 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. 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 \(p. 1006\)](#)
- [Grupos de segurança \(p. 1006\)](#)
- [Excluir no encerramento \(p. 1007\)](#)
- [Verificação de origem/destino \(p. 1007\)](#)

### 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 \(p. 1552\)](#).

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 \(p. 1004\)](#).

#### 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.

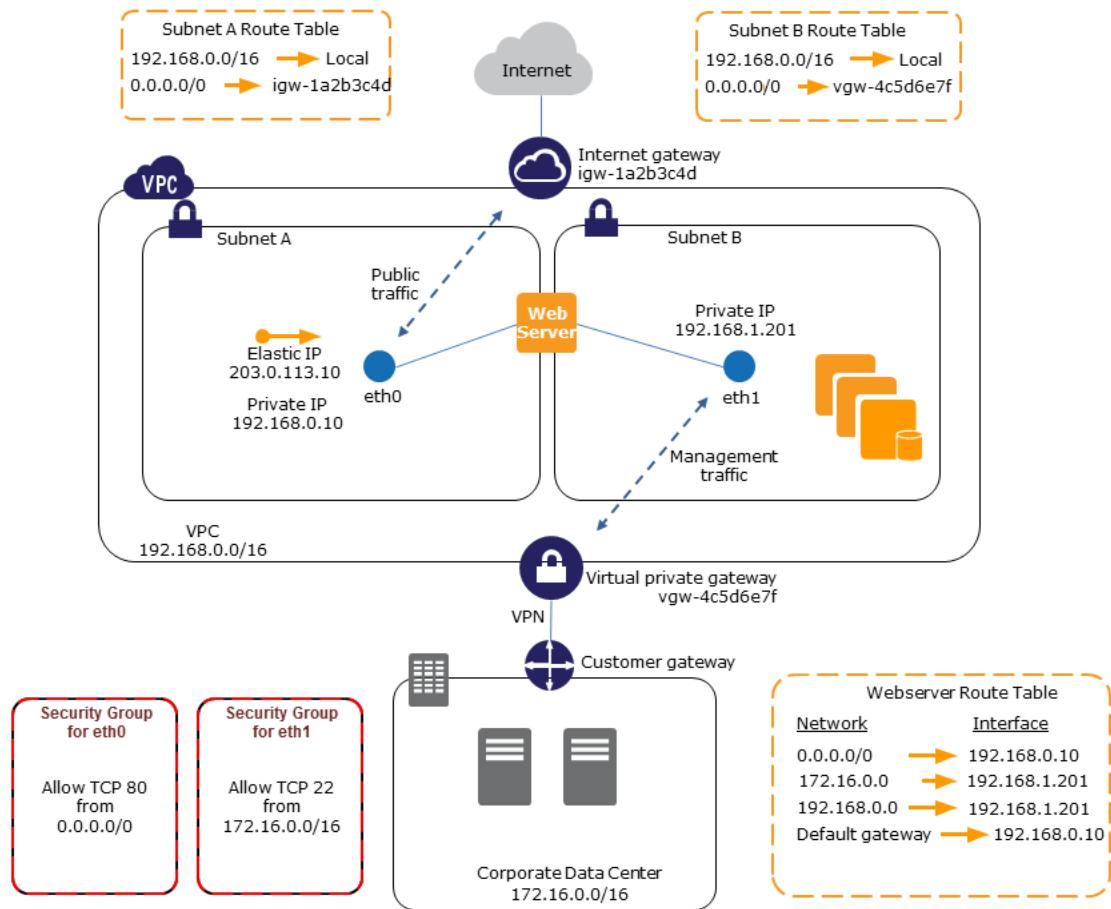
Você pode criar uma rede de gerenciamento usando interfaces de rede. Nesse cenário, conforme ilustrado na imagem a seguir:

- 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 SSH 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/funcões 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.

## Configurar a interface de rede usando ec2-net-utils

As AMIs do Amazon Linux podem conter scripts adicionais 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.

Use o comando instalar o pacote no Amazon Linux, caso ainda não esteja instalado, ou atualize-o se ele estiver instalado e houver atualizações adicionais disponíveis:

```
$ yum install ec2-net-utils
```

Os componentes a seguir fazem parte de ec2-net-utils:

Regras udev (/etc/udev/rules.d)

Identifica interfaces de rede quando são associadas, separadas ou religadas a uma instância em execução, e garante que o script de hotplug seja executado (53-ec2-network-interfaces.rules). Mapeia o endereço MAC para um nome de dispositivo (75-persistent-net-generator.rules, que gera 70-persistent-net.rules).

### Script de hotplug

Gera um arquivo de configuração de interface apropriado para uso com DHCP (/etc/sysconfig/network-scripts/ifcfg-ethN). Gera também um arquivo de configuração de rota (/etc/sysconfig/network-scripts/route-ethN).

### Script de DHCP

Sempre que a interface de rede receber um novo lease do DHCP, esse script consultará os metadados da instância para endereços IP elásticos. Para cada endereço IP elástico, ele adiciona uma regra ao banco de dados de políticas de roteamento para garantir que o tráfego de saída desse endereço use a interface de rede correta. Ele também adiciona cada endereço IP privado à interface de rede como um endereço secundário.

### ec2ifup ethN

Estende a funcionalidade de padrão ifup. Depois de o script reescrever os arquivos de configuração ifcfg-ethN e route-ethN, ele executará o ifup.

### ec2ifdown ethN

Estende a funcionalidade de padrão ifdown. Depois de o script eliminar todas as regras da interface de rede do banco de dados de políticas de roteamento, ele executará o ifdown.

### ec2ifscan

Verifica se há interfaces de rede que não foram configuradas e as configura.

Este script não está disponível na versão inicial de ec2-net-utils.

Para listar todos os arquivos de configuração gerados por ec2-net-utils, use o seguinte comando:

```
$ ls -l /etc/sysconfig/network-scripts/*-eth?
```

Para desabilitar a automação por instância, você pode adicionar EC2SYNC=no ao arquivo ifcfg-ethN correspondente. Por exemplo, use o comando a seguir para desabilitar a automação da interface eth1:

```
$ sed -i -e 's/^EC2SYNC=yes/EC2SYNC=no/' /etc/sysconfig/network-scripts/ifcfg-eth1
```

Para desativar completamente a automação, pode remover o pacote usando o seguinte comando:

```
$ yum remove ec2-net-utils
```

## 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 \(p. 1007\)](#).

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-c8fbcc27e",  
    "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 \(p. 204\)](#) 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 \(p. 1085\)](#) 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, `umm5.8xlarge` 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 \(p. 220\)](#)
- [Instâncias otimizadas para computação \(p. 273\)](#)
- [Instâncias otimizadas para memória \(p. 282\)](#)
- [Instâncias otimizadas para armazenamento \(p. 297\)](#)
- [Instâncias computacionais aceleradas \(p. 310\)](#)

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 \(p. 876\)](#)
- [Métricas de performance da rede \(p. 1032\)](#)

## Rede avançada no Linux

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 \(p. 1016\)](#). 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 \(p. 1016\)](#)
- [Habilitar redes avançadas na instância \(p. 1016\)](#)
- [Habilitar redes avançadas com o Elastic Network Adapter \(ENA\) em instâncias do Linux \(p. 1016\)](#)
- [Habilitar redes avançadas com a interface Intel 82599 VF nas instâncias do Linux \(p. 1026\)](#)
- [Otimizações do sistema operacional \(p. 1032\)](#)
- [Monitorar a performance de rede de sua instância do EC2 \(p. 1032\)](#)
- [Solução de problemas do Elastic Network Adapter \(ENA\) \(p. 1036\)](#)

## Suporte a redes avançadas

Todos os tipos de instância da [geração atual \(p. 204\)](#) 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 \(p. 211\)](#).

## 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 Linux \(p. 1016\)](#).

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 Linux \(p. 1026\)](#).

## Habilitar redes avançadas com o Elastic Network Adapter (ENA) em instâncias do Linux

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 \(p. 1017\)](#)
- [Performance da rede avançada \(p. 1017\)](#)
- [Testar se a rede avançada está habilitada \(p. 1017\)](#)
- [Para habilitar redes avançadas no Amazon Linux AMI \(p. 1019\)](#)
- [Para habilitar redes avançadas no Ubuntu \(p. 1020\)](#)
- [Para habilitar redes avançada no Linux \(p. 1022\)](#)
- [Habilitar redes avançadas no Ubuntu com DKMS \(p. 1024\)](#)
- [Notas de release do driver \(p. 1025\)](#)
- [Troubleshoot \(p. 1026\)](#)

## 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 \(p. 204\)](#) que seja diferente das instâncias C4, D2 e M4 menores do que m4.16xlarge ou T2.
- Execute a instância usando uma versão e uma distribuição compatíveis do kernel do Linux, para que as redes avançadas do ENA sejam habilitadas automaticamente para a instância. Para obter mais informações, consulte [Notas de release do driver ENA do kernel do Linux](#).
- 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 \(p. 310\)](#)
- [Performance de rede para instâncias otimizadas para computação \(p. 277\)](#)
- [Performance de rede para instâncias de uso geral \(p. 220\)](#)
- [Performance de rede para instâncias otimizadas para memória \(p. 289\)](#)
- [Performance de rede para instâncias otimizadas para armazenamento \(p. 300\)](#)

## Testar se a rede avançada está habilitada

As AMIs a seguir incluem o módulo ENA necessário e o suporte para ENA habilitado:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (com kernel `linux-aws`) ou posterior
- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior

Para testar se a rede avançada já está habilitada, verifique se o módulo `ena` está instalado na instância e se o atributo `enaSupport` está definido. Se a instância atender a essas duas condições, o comando `ethtool -i ethn` deve mostrar que o módulo está em uso na interface de rede.

Módulo de kernel (`ena`)

Para verificar se o módulo ena está instalado, use o comando modinfo conforme mostrado no exemplo a seguir.

```
[ec2-user ~]$ modinfo ena
filename:      /lib/modules/4.14.33-59.37.amzn2.x86_64/kernel/drivers/amazon/net/ena/
ena.ko
version:       1.5.0g
license:        GPL
description:   Elastic Network Adapter (ENA)
author:         Amazon.com, Inc. or its affiliates
srcversion:    692C7C68B8A9001CB3F31D0
alias:          pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:          pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:          pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:          pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
retpoline:     Y
intree:        Y
name:          ena
...
```

No caso do Amazon Linux acima, o módulo ena está instalado.

```
ubuntu:~$ modinfo ena
ERROR: modinfo: could not find module ena
```

Na instância do Ubuntu acima, o módulo não é instalado, portanto, primeiro você deve instalá-lo. Para obter mais informações, consulte [Para habilitar redes avançadas no Ubuntu \(p. 1020\)](#).

#### 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
```

#### Driver da interface de rede

Use o comando a seguir para verificar se o módulo ena está sendo usado em uma interface específica, substituindo o nome da interface que você deseja verificar. Se estiver usando uma única interface (padrão), ela será a eth0. Se o sistema operacional oferecer suporte a [nomes de rede previsíveis \(p. 1022\)](#), esse poderá ser um nome como ens5.

No exemplo acima, o módulo ena não está carregado porque o driver listado é vif.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Nesse exemplo, o módulo ena está carregado e na versão mínima recomendada. Essa instância configurou a rede avançada corretamente.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

## Para habilitar redes avançadas no Amazon Linux AMI

O Amazon Linux 2 e as versões mais recentes do Amazon Linux AMI incluem o módulo necessário para a rede aprimorada com o ENA instalado e o suporte para ENA habilitado. Portanto, se você executar uma instância com uma versão HVM do Amazon Linux em um tipo de instância compatível, a rede avançada já estará habilitada para a instância. Para obter mais informações, consulte [Testar se a rede avançada está habilitada \(p. 1017\)](#).

Se você executou a instância usando uma AMI do Amazon Linux mais antiga e ela ainda não tiver a rede avançada habilitada, use o seguinte procedimento para habilitar a rede avançada.

### Para habilitar a rede avançada na Amazon Linux AMI

1. Conecte-se à sua instância.
2. Na instância, execute o seguinte comando para atualizar a instância com o kernel e os módulos de kernel mais recentes incluindo ena:

```
[ec2-user ~]$ sudo yum update
```

3. No computador local, reinicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: [reboot-instances](#) (AWS CLI), [Restart-EC2Instance](#) (AWS Tools for Windows PowerShell).
4. Conecte-se à instância novamente e verifique se o módulo ena está instalado e na versão mínima recomendada usando o comando modinfo ena em [Testar se a rede avançada está habilitada \(p. 1017\)](#).
5. [Instância com EBS] 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.

[Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: [Para habilitar a rede avançada na Amazon Linux AMI \(instâncias compatíveis com o armazenamento de instâncias\) \(p. 1020\)](#).

6. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:

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

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute](#) (Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

7. (Opcional) Crie uma AMI na instância, conforme descrito em [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#). A AMI herda o atributo de rede avançada enaSupport 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.
9. Conecte-se à instância e verifique se o módulo ena está instalado e carregado na interface de rede usando o comando `ethtool -i ethn` em [Testar se a rede avançada está habilitada \(p. 1017\)](#).

Se não for possível conectar-se à instância depois de habilitar a rede avançada, consulte [Solução de problemas do Elastic Network Adapter \(ENA\) \(p. 1036\)](#).

Para habilitar a rede avançada na Amazon Linux AMI (instâncias compatíveis com o armazenamento de instâncias)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

## Para habilitar redes avançadas no Ubuntu

As AMIs do HVM do Ubuntu mais recentes incluem o módulo necessário para a rede aprimorada com o ENA instalado e o suporte para ENA habilitado. Portanto, se você executar uma instância com a AMI do HVM do Ubuntu mais recente em um tipo de instância compatível, a rede avançada já estará habilitada para a instância. Para obter mais informações, consulte [Testar se a rede avançada está habilitada \(p. 1017\)](#).

Se tiver executado a instância usando uma AMI mais antiga e ela ainda não tiver as redes avançadas habilitadas, você poderá instalar o pacote do kernel `linux-aws` para obter os drivers de redes avançadas mais recentes e atualizar o atributo necessário.

Para instalar o pacote do kernel **linux-aws** (Ubuntu 16.04 ou posterior)

O Ubuntu 16.04 e o 18.04 são fornecidos com o kernel personalizado do Ubuntu (pacote do kernel **linux-aws**). Para usar um kernel diferente, entre em contato com o [AWS Support](#).

Para instalar o pacote do kernel **linux-aws** (Ubuntu Trusty 14.04)

1. Conecte-se à sua instância.
2. Atualize o cache de pacotes e os pacotes.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

#### Important

Se, durante o processo de atualização, for solicitada a instalação do grub, use o `/dev/xvda` para instalar o grub e, em seguida, escolha manter a versão atual do `/boot/grub/menu.lst`.

3. [Instância com EBS] 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.

[Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: [Para habilitar a rede avançada no Ubuntu \(instâncias com suporte do armazenamento de instâncias\) \(p. 1021\)](#).

4. No computador local, ative o atributo de rede avançada usando um dos seguintes comandos:
  - [modify-instance-attribute](#) (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute](#) (Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

5. (Opcional) Crie uma AMI na instância, conforme descrito em [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#). A AMI herda o atributo de rede avançada enaSupport da instância. Portanto, você pode usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.
6. 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.

Para habilitar a rede avançada no Ubuntu (instâncias com suporte do armazenamento de instâncias)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

## Para habilitar redes avançada no Linux

As AMIs mais recentes para Red Hat Enterprise Linux, SUSE Linux Enterprise Server e CentOS incluem o módulo necessário para redes aprimoradas com ENA e o suporte para ENA habilitado. Portanto, se você executar uma instância com a AMI mais recente em um tipo de instância compatível, a rede aprimorada já estará habilitada para a instância. Para obter mais informações, consulte [Testar se a rede avançada está habilitada \(p. 1017\)](#).

O procedimento a seguir fornece as etapas gerais para habilitar a rede aprimorada em uma distribuição do Linux diferente do Amazon Linux AMI ou do Ubuntu. Para obter mais informações, como a sintaxe detalhada dos comandos, os locais dos arquivos ou o suporte para o pacote e a ferramenta, consulte a documentação da sua distribuição do Linux.

### Para habilitar a rede avançada no Linux

1. Conecte-se à sua instância.
2. Clone o código-fonte do módulo ena na instância a partir do GitHub em <https://github.com/amzn/amzn-drivers>. (Como o SUSE Linux Enterprise Server 12 SP2 e posterior incluem ENA 2.02 por padrão, não é necessário fazer download e compilar o driver ENA. Para o SUSE Linux Enterprise Server 12 SP2 e posterior, você deve registrar uma solicitação para adicionar a versão do driver que deseja ao kernel comercial).

```
git clone https://github.com/amzn/amzn-drivers
```

3. Compile e instale o módulo ena na instância. Essas etapas dependem da distribuição Linux. Para obter mais informações sobre como compilar o módulo no Red Hat Enterprise Linux, consulte o [Artigo da Central de Conhecimento da AWS](#).
4. Execute o comando sudo depmod para atualizar as dependências do módulo.
5. Atualize o `initramfs` na instância para garantir que o novo módulo seja carregado na hora da inicialização. Por exemplo, se a distribuição oferecer suporte a dracut, você poderá usar o comando a seguir.

```
dracut -f -v
```

6. Determine se o sistema usa nomes previsíveis de interface de rede por padrão. Os sistemas que usam as versões 197 ou superiores do systemd ou udev podem renomear dispositivos de Ethernet e não garantem que uma única interface de rede será nomeada `eth0`. Esse comportamento pode causar problemas para conexão à instância. Para mais informações e ver outras opções de configuração, consulte [Nomes previsíveis de interface de rede](#) no site freedesktop.org.
  - a. É possível verificar as versões do systemd ou udev em sistemas baseados em RPM com o comando a seguir.

```
rpm -qa | grep -e '^systemd-[0-9]+\|^udev-[0-9]+\+'  
systemd-208-11.el7_0.2.x86_64
```

No exemplo do Red Hat Enterprise Linux 7 acima, a versão do systemd é a 208, portanto, os nomes previsíveis de interface de rede devem ser desativados.

- b. Desabilite nomes previsíveis de interface de rede adicionando a opção `net.ifnames=0` à linha `GRUB_CMDLINE_LINUX` no `/etc/default/grub`.

```
sudo sed -i '/^GRUB_CMDLINE_LINUX/s/$/\ net.ifnames=0"/' /etc/default/grub
```

- c. Recompile o arquivo de configuração do grub.

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Instância com EBS] 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.

[Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: [Para habilitar as redes avançadas no Linux \(instâncias compatíveis com o armazenamento de instância\)](#) (p. 1023).

8. No computador local, ative o atributo de rede avançada `enaSupport` usando um dos seguintes comandos:

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

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- [Edit-EC2InstanceAttribute](#) (Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
```

9. (Opcional) Crie uma AMI na instância, conforme descrito em [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#). A AMI herda o atributo de rede avançada `enaSupport` da instância. Portanto, você pode usar essa AMI para executar outra instância com a rede avançada habilitada por padrão.

**Important**

Se o sistema operacional da instância contiver um arquivo `/etc/udev/rules.d/70-persistent-net.rules`, você deverá excluí-lo antes de criar a AMI. Esse arquivo contém o endereço MAC do adaptador de Ethernet da instância original. Se outra instância for iniciada com esse arquivo, o sistema operacional será incapaz de localizar o dispositivo e o `eth0` poderá falhar causando problemas de inicialização. Esse arquivo é gerado novamente no próximo ciclo de inicialização, e todas as instâncias executadas na AMI criam sua própria versão do arquivo.

10. 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.
11. (Opcional) Conecte-se à instância e verifique se o módulo está instalado.

Se não for possível conectar-se à instância depois de habilitar a rede avançada, consulte [Solução de problemas do Elastic Network Adapter \(ENA\)](#) (p. 1036).

Para habilitar as redes avançadas no Linux (instâncias compatíveis com o armazenamento de instância)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em [Criar uma AMI em Linux com armazenamento de instâncias](#) (p. 112), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image](#) (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- [Register-EC2Image \(AWS Tools for Windows PowerShell\)](#)

```
Register-EC2Image -EnaSupport ...
```

## Habilitar redes avançadas no Ubuntu com DKMS

Esse método é apenas para fins de teste e feedback. Não é destinado ao uso com implantações de produção. Para implantações de produção, consulte [Para habilitar redes avançadas no Ubuntu \(p. 1020\)](#).

### Important

O uso do DKMS anula o acordo de suporte da sua assinatura. Ele não deve ser usado para implantações de produção.

Para habilitar a rede avançada com o ENA no Ubuntu (instâncias com suporte do EBS)

1. Siga as etapas 1 e 2 em [Para habilitar redes avançadas no Ubuntu \(p. 1020\)](#).
2. Instale os pacotes do build-essential para compilar o módulo de kernel e o pacote dkms para que o módulo ena seja recompilado sempre que o kernel for atualizado.

```
ubuntu:~$ sudo apt-get install -y build-essential dkms
```

3. Clone a fonte do módulo ena na instância a partir do GitHub em <https://github.com/amzn/amzn-drivers>.

```
ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
```

4. Mova o pacote amzn-drivers para o diretório /usr/src/ para que o DKMS possa localizá-lo e compilá-lo para cada atualização de kernel. Adicione o número da versão (você pode localizar o número da versão atual nas notas de release) do código-fonte ao nome do diretório. Por exemplo, a versão 1.0.0 é mostrada no exemplo a seguir.

```
ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
```

5. Crie o arquivo de configuração do DKMS com os valores a seguir substituindo a versão do ena.

Criar o arquivo.

```
ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
```

Edito o arquivo e adicione os valores a seguir.

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Adicione, compile e instale o módulo ena na instância usando o DKMS.

Adicione o módulo ao DKMS.

```
ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
```

Compile o módulo usando o comando dkms.

```
ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
```

Instale o módulo usando o dkms.

```
ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
```

7. Compile o initramfs novamente para que o módulo correto seja carregado na hora da inicialização.

```
ubuntu:~$ sudo update-initramfs -u -k all
```

8. Verifique se o módulo ena está instalado usando o comando modinfo ena em [Testar se a rede avançada está habilitada \(p. 1017\)](#).

```
ubuntu:~$ modinfo ena
filename:      /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
version:       1.0.0
license:       GPL
description:   Elastic Network Adapter (ENA)
author:        Amazon.com, Inc. or its affiliates
srcversion:    9693C876C54CA64AE48FOCA
alias:         pci:v00001D0FD0000EC21sv*sd*bc*sc*i*
alias:         pci:v00001D0FD0000EC20sv*sd*bc*sc*i*
alias:         pci:v00001D0FD00001EC2sv*sd*bc*sc*i*
alias:         pci:v00001D0FD00000EC2sv*sd*bc*sc*i*
depends:
vermagic:     3.13.0-74-generic SMP mod_unload modversions
parm:          debug:Debug level (0=none,...,16=all) (int)
parm:          push_mode:Descriptor / header push mode
              (0=automatic,1=disable,3=enable)
              0 - Automatically choose according to device capability (default)
              1 - Don't push anything to device memory
              3 - Push descriptors and header buffer to device memory (int)
parm:          enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1)
              (int)
parm:          enable_missing_tx_detection:Enable missing Tx completions. (default=1)
              (int)
parm:          numa_node_override_array:Numa node override map
              (array of int)
parm:          numa_node_override:Enable/Disable numa node override (0=disable)
              (int)
```

9. Passe para a etapa 3 em [Para habilitar redes avançadas no Ubuntu \(p. 1020\)](#).

## Notas de release do driver

Para obter informações sobre as versões do driver do ENA para Linux, consulte as [notas de release do driver do kernel do ENA para Linux](#).

## Troubleshoot

Para obter informações sobre a solução de problemas, consulte [Solução de problemas do Elastic Network Adapter \(ENA\) \(p. 1036\)](#).

# Habilitar redes avançadas com a interface Intel 82599 VF nas instâncias do Linux

O Amazon EC2 fornece recursos de redes avançadas por meio da interface Intel 82599 VF, que usa o driver `ixgbevf` da Intel.

### Tópicos

- [Requirements \(p. 1026\)](#)
- [Testar se a rede avançada está habilitada \(p. 1026\)](#)
- [Habilitar a rede avançada no Amazon Linux \(p. 1028\)](#)
- [Para habilitar redes avançadas no Ubuntu \(p. 1029\)](#)
- [Habilitar redes avançadas em outras distribuições do Linux \(p. 1030\)](#)
- [Solucionar problemas de conectividade \(p. 1032\)](#)

## 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.
- Execute a instância de uma AMI de HVM usando uma versão de kernel do Linux de 2.6.32 ou superior. As AMIs HVM do Amazon Linux mais recentes têm os módulos necessários para a rede avançada instalada e também têm os atributos necessários definidos. Portanto, se você executar uma instância compatível com redes avançadas com Amazon EBS que usa uma AMI de HVM do Amazon Linux, a rede avançada já estará habilitada para a instância.

### Warning

A rede avançada é compatível apenas com instâncias de HVM. A habilitação da rede avançada com uma instância PV pode torná-la inacessível. A configuração desse atributo sem o módulo ou a versão do módulo adequados também pode tornar a instância inacessível.

- 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 módulo `ixgbevf` estiver instalado na instância e se o atributo `sriovNetSupport` está definido.

#### Atributo de instância (srivNetSupport)

Para verificar se uma instância tem o atributo `srivNetSupport` 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 srivNetSupport
```

- [Get-EC2InstanceAttribute](#) (AWS Tools for Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance_id -Attribute srivNetSupport
```

Se o atributo não estiver definido, o `SrivNetSupport` estará vazio. Se o atributo for definido, o valor será simples, como mostrado na saída de exemplo a seguir.

```
"SrivNetSupport": {  
    "Value": "simple"  
},
```

#### Atributo de imagem (srivNetSupport)

Para verificar se uma AMI já tem o atributo `srivNetSupport` 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[].[SrivNetSupport]"
```

- [Get-EC2Image](#) (AWS Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami_id).SrivNetSupport
```

Se o atributo não estiver definido, o `SrivNetSupport` estará vazio. Se o atributo for definido, o valor será simples.

#### Driver da interface de rede

Use o comando a seguir para verificar se o módulo está sendo usado em uma interface específica, substituindo o nome da interface que você deseja verificar. Se estiver usando uma única interface (padrão), ela será `eth0`. Se o sistema operacional oferecer suporte a [nomes de rede previsíveis](#) (p. 1030), esse poderá ser um nome como `ens5`.

No exemplo acima, o módulo `ixgbevf` não está carregado porque o driver listado é `vif`.

```
[ec2-user ~]$ ethtool -i eth0  
driver: vif  
version:  
firmware-version:  
bus-info: vif-0  
supports-statistics: yes  
supports-test: no  
supports-eeprom-access: no  
supports-register-dump: no  
supports-priv-flags: no
```

Nesse exemplo, o módulo `ixgbevf` está carregado. Essa instância configurou a rede avançada corretamente.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

## Habilitar a rede avançada no Amazon Linux

As AMIs de HVM do Amazon Linux têm o módulo `ixgbevf` necessário para a rede avançada instalado e também têm o atributo necessário `sriovNetSupport` definido. Portanto, se você executar um tipo de instância que use uma AMI de HVM do Amazon Linux, a rede avançada já estará habilitada para a instância. Para obter mais informações, consulte [Testar se a rede avançada está habilitada \(p. 1026\)](#).

Se você executou a instância usando uma AMI do Amazon Linux mais antiga e ela ainda não tiver a rede avançada habilitada, use o seguinte procedimento para habilitar a rede avançada.

### 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.
2. Na instância, execute o seguinte comando para atualizar a instância com o kernel e os módulos de kernel mais recentes incluindo `ixgbevf`:

```
[ec2-user ~]$ sudo yum update
```

3. No computador local, reinicie a instância usando o console do Amazon EC2 ou um dos seguintes comandos: [reboot-instances](#) (AWS CLI), [Restart-EC2Instance](#) (AWS Tools for Windows PowerShell).
4. Conecte-se à instância novamente e verifique se o módulo `ixgbevf` está instalado e na versão mínima recomendada usando o comando `modinfo ixgbevf` em [Testar se a rede avançada está habilitada \(p. 1026\)](#).
5. [Instância com EBS] 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.

[Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: [Para habilitar a rede avançada \(instâncias compatíveis com o armazenamento de instâncias\) \(p. 1029\)](#).

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 --sriov-net-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 Linux baseada em Amazon EBS \(p. 107\)](#). 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.
9. Conecte-se à instância e verifique se o módulo `ixgbevf` está instalado e carregado na interface de rede usando o comando `ethtool -i ethn` em [Testar se a rede avançada está habilitada \(p. 1026\)](#).

Para habilitar a rede avançada (instâncias compatíveis com o armazenamento de instâncias)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image](#) (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

## Para habilitar redes avançadas no Ubuntu

Antes de começar, o [verifica se a rede avançada já está habilitada \(p. 1026\)](#) em sua instância.

As AMIs do Ubuntu HVM Quick Start incluem os drivers necessários para redes aprimoradas. Se você tiver uma versão de `ixgbevf` anterior a 2.16.4, poderá instalar o `linux-aws` pacote do kernel para obter os drivers de rede aprimorados mais recentes.

O procedimento a seguir fornece as etapas gerais para compilar o módulo `ixgbevf` em uma instância do Ubuntu.

Para instalar o pacote do kernel `linux-aws`

1. Conecte-se à sua instância.
2. Atualize o cache de pacotes e os pacotes.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

### Important

Se, durante o processo de atualização, for solicitada a instalação do grub, use o `/dev/xvda` para instalar o grub e, em seguida, escolha manter a versão atual do `/boot/grub/menu.lst`.

## Habilitar redes avançadas em outras distribuições do Linux

Antes de começar, o [verifica se a rede avançada já está habilitada \(p. 1026\)](#) em sua instância. As AMIs do HVM Quick Start mais recentes incluem os drivers necessários para rede avançada, portanto, você não precisa executar etapas adicionais.

O procedimento a seguir fornece as etapas gerais se precisar habilitar a rede avançada com a interface Intel 82599 VF em uma distribuição do Linux diferente do Amazon Linux ou do Ubuntu. Para obter mais informações, como a sintaxe detalhada dos comandos, os locais dos arquivos ou suporte para o pacote e a ferramenta, consulte a documentação específica à sua distribuição do Linux.

Para habilitar a rede avançada no Linux

1. Conecte-se à sua instância.
2. Faça download da fonte para o módulo `ixgbevf` na instância do Sourceforge em <https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/>.

Versões do `ixgbevf` anteriores à 2.16.4, incluindo a versão 2.14.2, não são compiladas adequadamente em algumas distribuições do Linux, incluindo certas versões do Ubuntu.

3. Compile e instale o módulo `ixgbevf` na instância.

### Warning

Se você compilar o módulo `ixgbevf` para o kernel atual e, depois, atualizar o kernel sem recompilar o driver para o novo kernel, o sistema poderá reverter o módulo `ixgbevf` específico à distribuição na próxima reinicialização. Isso poderá tornar o sistema inacessível se a versão específica à distribuição for incompatível com a rede avançada.

4. Execute o comando `sudo depmod` para atualizar as dependências do módulo.
5. Atualize o `initramfs` na instância para garantir que o novo módulo seja carregado na hora da inicialização.
6. Determine se o sistema usa nomes previsíveis de interface de rede por padrão. Os sistemas que usam as versões 197 ou superiores do `systemd` ou `udev` podem renomear dispositivos de Ethernet e não garantem que uma única interface de rede será nomeada `eth0`. Esse comportamento pode causar problemas para conexão à instância. Para mais informações e ver outras opções de configuração, consulte [Nomes previsíveis de interface de rede](#) no site freedesktop.org.
  - a. Você pode verificar as versões do `systemd` ou `udev` em sistemas baseados em RPM com o seguinte comando:

```
[ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]+\+|^\udev-[0-9]+\+'  
systemd-208-11.el7_0.2.x86_64
```

No exemplo do Red Hat Enterprise Linux 7 acima, a versão do `systemd` é a 208, portanto, os nomes previsíveis de interface de rede devem ser desativados.

- b. Desabilite nomes previsíveis de interface de rede adicionando a opção `net.ifnames=0` à linha `GRUB_CMDLINE_LINUX` no `/etc/default/grub`.

```
[ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/ \ net\.ifnames\=0\"/' /etc/  
default/grub
```

- c. Recompile o arquivo de configuração do grub.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [Instância com EBS] 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.

[Instância baseada em armazenamento de instâncias] Você não pode parar a instância para modificar o atributo. Em vez disso, siga este procedimento: [Para habilitar as redes avançadas \(instâncias compatíveis com o armazenamento de instância\) \(p. 1031\)](#).

- 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"
```

- (Opcional) Crie uma AMI na instância, conforme descrito em [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#). 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.

#### Important

Se o sistema operacional da instância contiver um arquivo `/etc/udev/rules.d/70-persistent-net.rules`, você deverá excluí-lo antes de criar a AMI. Esse arquivo contém o endereço MAC do adaptador de Ethernet da instância original. Se outra instância for iniciada com esse arquivo, o sistema operacional será incapaz de localizar o dispositivo e o `eth0` poderá falhar causando problemas de inicialização. Esse arquivo é gerado novamente no próximo ciclo de inicialização, e todas as instâncias executadas na AMI criam sua própria versão do arquivo.

- 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.
- (Opcional) Conecte-se à instância e verifique se o módulo está instalado.

Para habilitar as redes avançadas (instâncias compatíveis com o armazenamento de instância)

Siga o procedimento anterior até a etapa onde você para a instância. Crie uma nova AMI como descrito em [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#), habilitando o atributo de rede avançada ao registrar a AMI.

- [register-image](#) (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --srivnet-support simple ...
```

- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

## Solucionar problemas de conectividade

Se você perder a conectividade ao habilitar a rede avançada, o módulo `ixgbevf` talvez seja incompatível com o kernel. Tente instalar a versão do módulo `ixgbevf` incluída com a distribuição do Linux para a instância.

Se você habilitar a rede avançada para uma instância de PV ou de AMI, poderá tornar a instância inatingível.

Para obter mais informações, consulte [Como habilitar e configurar as redes avançadas em minhas instâncias do EC2?](#).

## 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. Para obter mais informações, consulte o [Guia de Práticas Recomendadas e Otimização de Performance do Driver](#) no github.

## 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 \(p. 1033\)](#)

- [Métricas para o driver ENA \(p. 1033\)](#)
- [Exibir as métricas de performance de rede para sua instância do Linux \(p. 1034\)](#)
- [Métricas de performance de rede com o driver DPDK para ENA \(p. 1034\)](#)
- [Métricas em instâncias que executam o FreeBSD \(p. 1035\)](#)

## Requirements

Os seguintes requisitos se aplicam às instâncias do Linux.

- Instale o driver ENA versão 2.2.10 ou posterior. Para verificar a versão instalada, use o comando ethtool. No exemplo a seguir, a versão atende ao requisito mínimo.

```
[ec2-user ~]$ ethtool -i eth0 | grep version
version: 2.2.10
```

Para atualizar seu driver ENA, consulte [Redes avançadas \(p. 1016\)](#).

- Para importar essas métricas para o Amazon CloudWatch, instale o agente CloudWatch. Para obter mais informações, consulte [Coletar métricas de performance 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.

As métricas a seguir estão disponíveis em instâncias Linux, instâncias FreeBSD e ambientes DPDK.

Métrica	Descrição
<code>bw_in_allowance_exceeded</code>	Número de pacotes na fila ou descartados porque a largura de banda agregada de entrada excedeu o máximo para a instância.
<code>bw_out_allowance_exceeded</code>	Número de pacotes na fila ou descartados porque a largura de banda agregada de saída excedeu o máximo para a instância.
<code>conntrack_allowance_exceeded</code>	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.
<code>linklocal_allowance_exceeded</code>	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.
<code>pps_allowance_exceeded</code>	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 Linux

Você pode publicar métricas em suas ferramentas favoritas para visualizar os dados das métricas. Por exemplo, você pode publicar as métricas em Amazon CloudWatch usando o agente CloudWatch. O agente permite que você selecione métricas individuais e controle a publicação.

Você também pode usar o ethtool para recuperar as métricas para cada interface de rede, como eth0, conforme mostrado a seguir.

```
[ec2-user ~]$ ethtool -S eth0
bw_in_allowance_exceeded: 0
bw_out_allowance_exceeded: 0
pps_allowance_exceeded: 0
conntrack_allowance_exceeded: 0
linklocal_allowance_exceeded: 0
```

## Métricas de performance de rede com o driver DPDK para ENA

O driver ENA versão 2.2.0 e posterior oferece suporte a relatórios de métricas de rede. O DPDK 20.11 inclui o driver ENA 2.2.0 e é a primeira versão do DPDK a suportar esse recurso.

Você pode usar uma aplicação de exemplo para exibir estatísticas DPDK. Para iniciar uma versão interativa da aplicação de exemplo, execute o seguinte comando.

```
./app/dpdk-testpmd -- -i
```

Dentro desta sessão interativa, você pode inserir um comando para recuperar dados estatísticos estendidos para uma porta. O comando de exemplo a seguir recupera as estatísticas da porta 0.

```
show port xstats 0
```

Veja a seguir um exemplo de uma sessão interativa com a aplicação de exemplo DPDK.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
EAL: Detected 4 lcore(s)
EAL: Detected 1 NUMA nodes
EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
EAL: Selected IOVA mode 'PA'
EAL: Probing VFIO support...
EAL: Invalid NUMA socket, default to 0
EAL: Invalid NUMA socket, default to 0
EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
EAL: No legacy callbacks, legacy socket not created
Interactive-mode selected

Port 0: link state change event
testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
testpmd: preferred mempool ops selected: ring_mp_mc

Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

Configuring Port 0 (socket 0)
Port 0: 02:C7:17:A2:60:B1
Checking link statuses...
```

```
Done
Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
testpmd> show port xstats 0
##### NIC extended statistics for port 0
rx_good_packets: 0
tx_good_packets: 0
rx_good_bytes: 0
tx_good_bytes: 0
rx_missed_errors: 0
rx_errors: 0
tx_errors: 0
rx_mbuf_allocation_errors: 0
rx_q0_packets: 0
rx_q0_bytes: 0
rx_q0_errors: 0
tx_q0_packets: 0
tx_q0_bytes: 0
wd_expired: 0
dev_start: 1
dev_stop: 0
tx_drops: 0
bw_in_allowance_exceeded: 0
bw_out_allowance_exceeded: 0
pps_allowance_exceeded: 0
conntrack_allowance_exceeded: 0
linklocal_allowance_exceeded: 0
rx_q0_cnt: 0
rx_q0_bytes: 0
rx_q0_refill_partial: 0
rx_q0_bad_csum: 0
rx_q0_mbuf_alloc_fail: 0
rx_q0_bad_desc_num: 0
rx_q0_bad_req_id: 0
tx_q0_cnt: 0
tx_q0_bytes: 0
tx_q0_prepare_ctx_err: 0
tx_q0_linearize: 0
tx_q0_linearize_failed: 0
tx_q0_tx_poll: 0
tx_q0_doorbells: 0
tx_q0_bad_req_id: 0
tx_q0_available_desc: 1023
testpmd>
```

Para obter mais informações sobre a aplicação de exemplo e usá-lo para recuperar dados estatísticos estendidos, consulte [Guia do usuário da aplicação Testpmd](#) na documentação do DPDK.

## Métricas em instâncias que executam o FreeBSD

A partir da versão 2.3.0, o driver ENA FreeBSD suporta a coleta de métricas de performance de rede em instâncias que executam o FreeBSD. Para habilitar a coleção de métricas do FreeBSD, insira o seguinte comando e defina o **intervalo** como um valor entre 1 e 3.600. Isso especifica com que frequência, em segundos, serão coletadas métricas do FreeBSD.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Por exemplo, o comando a seguir define o driver para coletar métricas do FreeBSD na interface de rede 1 a cada 10 segundos:

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Para desativar a coleção de métricas do FreeBSD, você pode executar o comando anterior e especificar 0 como [intervalo](#).

Depois de coletar métricas do FreeBSD, você poderá recuperar o conjunto mais recente de métricas coletadas executando o seguinte comando.

```
sysctl dev.ena.network\_interface.en1_metrics
```

## Solução de problemas do Elastic Network Adapter (ENA)

O Elastic Network Adapter (ENA) é projetado para melhorar a integridade do sistema operacional e reduzir as possibilidades de interrupção de longo prazo por conta de comportamento inesperado de hardware e/ou falhas. A arquitetura do ENA mantém falhas do dispositivo ou do driver o mais transparentes possível para o sistema. Este tópico fornece informações de solução de problemas para o ENA.

Caso você não consiga se conectar à sua instância, comece com a seção [Solucionar problemas de conectividade \(p. 1036\)](#).

Se você for capaz de se conectar à sua instância, pode coletar informações de diagnóstico usando os mecanismos de detecção e recuperação de falhas, cobertos nas seções posteriores deste tópico.

### Tópicos

- [Solucionar problemas de conectividade \(p. 1036\)](#)
- [Mecanismo de keep-alive \(p. 1037\)](#)
- [Registre o tempo limite de leitura \(p. 1038\)](#)
- [Statistics \(p. 1038\)](#)
- [Logs de erro do driver no syslog \(p. 1043\)](#)

## Solucionar problemas de conectividade

Se você perder a conectividade ao habilitar a rede avançada, o módulo ena talvez seja incompatível com o kernel atualmente em execução na sua instância. Isso pode acontecer se você instalar o módulo para uma versão específica do kernel (sem dkms ou com um arquivo dkms.conf configurado indevidamente) e o kernel da instância for atualizado. Se o kernel da instância que estiver carregado no momento da inicialização não tiver o módulo ena corretamente instalado, sua instância não reconhecerá o adaptador de rede e sua instância ficará inacessível.

Se você habilitar a rede avançada para uma instância de PV ou AMI, isso também poderá tornar a instância inatingível.

Se sua instância tornar-se inacessível após habilitar a rede avançada com ENA, você pode desabilitar o atributo `enaSupport` para sua instância e cairá no adaptador de rede em estoque.

Para desabilitar a rede avançada com ENA (instâncias com suporte do EBS)

1. 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.

#### Important

Se estiver usando uma instância com armazenamento de instâncias, você não poderá parar a instância. Em vez disso, prossiga para [Para desabilitar a rede avançada com o ENA \(instâncias com suporte do armazenamento de instâncias\) \(p. 1037\)](#).

2. No computador local, desative o atributo de rede avançada usando um comando a seguir.
  - [modify-instance-attribute](#) (AWS CLI)

```
$ aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
```
3. 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.
4. (Opcional) Conecte-se à sua instância e tente reinstalar o módulo ena com a versão atual do kernel seguindo as etapas em [Habilitar redes avançadas com o Elastic Network Adapter \(ENA\) em instâncias do Linux \(p. 1016\)](#).

Para desabilitar a rede avançada com o ENA (instâncias com suporte do armazenamento de instâncias)

Se sua instância for com armazenamento de instâncias, crie uma nova AMI como descrito em [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#). Desabilite o atributo de rede avançada enaSupport ao registrar a AMI.

- [register-image](#) (AWS CLI)

```
$ aws ec2 register-image --no-ena-support ...
```

- [Register-EC2Image](#) (AWS Tools for Windows PowerShell)

```
C:\> Register-EC2Image -EnaSupport $false ...
```

## Mecanismo de keep-alive

O dispositivo ENA posta eventos de keep-alive em uma taxa fixa (geralmente uma vez por segundo). O driver ENA implanta um mecanismo de watchdog, que verifica a presença dessas mensagens keep-alive. Se as mensagens estiverem presentes, o watchdog será rearmado; caso contrário, o driver concluirá que o dispositivo experimentou uma falha e fará o seguinte:

- Despejará as estatísticas atuais no syslog
- Redefinirá o dispositivo ENA
- Redefinirá o estado do driver do ENA

O procedimento de redefinição acima pode resultar em alguma perda de tráfego por um breve período (conexões TCP devem ser capazes recuperar), mas não deve afetar o usuário de outras formas.

O dispositivo ENA também pode indiretamente solicitar um procedimento de redefinição do dispositivo ao não enviar uma notificação de keep-alive, por exemplo, se o dispositivo ENA atingir um estado desconhecido depois de carregar uma configuração irrecuperável.

Abaixo está um exemplo do procedimento de redefinição:

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
```

```
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.....
.....
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the end
of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The driver
begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date [Wed
Apr 6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset process
is complete
```

## Registre o tempo limite de leitura

A arquitetura de ENA sugere um uso específico limitado de operações de leitura de E/S (MMIO) mapeadas de memória. Os registros de MMIO são acessados pelo driver do dispositivo ENA somente durante o procedimento de inicialização.

Se os logs do driver (disponíveis na saída do dmesg) indicarem falhas nas operações de leitura, isso pode ser causado por um driver incompatível ou incorretamente compilado, um dispositivo de hardware ocupado ou falha de hardware.

As entradas intermitentes do log que indicam falhas nas operações de leitura não devem ser consideradas um problema; o driver fará novas tentativas nesse caso. Contudo, uma sequência de entradas de log contendo falhas de leitura indica problema de driver ou de hardware.

Abaixo está um exemplo de entrada de log do driver indicando falha na operação de leitura devido a um tempo limite:

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout. expected:
req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout. expected:
req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

## Statistics

Se você tiver problemas de latência ou de performance de rede insuficiente, recupere as estatísticas dos dispositivos e examine-as. Essas estatísticas podem ser obtidas usando ethtool, como mostrado abaixo:

```
[ec2-user ~]$ ethtool -S ethN
```

```
NIC statistics:  
tx_timeout: 0  
suspend: 0  
resume: 0  
wd_expired: 0  
interface_up: 1  
interface_down: 0  
admin_q_pause: 0  
bw_in_allowance_exceeded: 0  
bw_out_allowance_exceeded: 0  
pps_allowance_exceeded: 0  
conntrack_allowance_exceeded: 0  
linklocal_allowance_exceeded: 0  
queue_0_tx_cnt: 4329  
queue_0_tx_bytes: 1075749  
queue_0_tx_queue_stop: 0  
...
```

Os parâmetros de saída de comando a seguir estão descritos abaixo:

**tx\_timeout:** *N*

O número de vezes que o watchdog Netdev foi ativado.

**suspend:** *N*

O número de vezes que o driver realizou uma operação de suspensão.

**resume:** *N*

O número de vezes que o driver realizou uma operação de retomada.

**wd\_expired:** *N*

O número de vezes que o driver não recebeu o evento de keep-alive nos três segundos anteriores.

**interface\_up:** *N*

O número de vezes que a interface do ENA foi ativada.

**interface\_down:** *N*

O número de vezes que a interface do ENA foi desativada.

**admin\_q\_pause:** *N*

O número de vezes que a fila do administrador não foi encontrada em um estado de execução.

**bw\_in\_allowance\_exceeded:** *N*

O número de pacotes rx descartados porque o limite da franquia da largura de banda foi excedido.

**bw\_out\_allowance\_exceeded:** *N*

O número de pacotes tx descartados porque o limite da franquia da largura de banda foi excedido.

**pps\_allowance\_exceeded:** *N*

O número de pacotes descartados porque o limite da franquia de pps (pacotes por segundo) foi excedido.

**conntrack\_allowance\_exceeded:** *N*

O número de pacotes descartados porque o limite da franquia da conta de conexão foi excedido.

**linklocal\_allowance\_exceeded:** *N*

O número de pacotes de proxy descartados porque o limite da franquia de pps (pacotes por segundo) foi excedido.

`queue_N_tx_cnt: N`

O número de pacotes transmitidos para essa fila.

`queue_N_tx_bytes: N`

O número de bytes transmitidos para essa fila.

`queue_N_tx_queue_stop: N`

O número de vezes em que a fila `N` estava cheia e interrompida.

`queue_N_tx_queue_wakeup: N`

O número de vezes que a fila `N` foi retomada depois de ser interrompida.

`queue_N_tx_dma_mapping_err: N`

Contagem de erro de acesso da memória direta. Se esse valor não for 0, isso indica recursos de sistema baixos.

`queue_N_tx_linearize: N`

O número de vezes que a linearização de SKB foi tentada para essa fila.

`queue_N_tx_linearize_failed: N`

O número de vezes que a linearização de SKB apresentou falha para essa fila.

`queue_N_tx_napi_comp: N`

O número de vezes que o manipulador `napi` chamou `napi_complete` para essa fila.

`queue_N_tx_tx_poll: N`

O número de vezes que o manipulador `napi` foi programado para essa fila.

`queue_N_tx_doorbells: N`

O número de campainhas de transmissão para essa fila.

`queue_N_tx_prepare_ctx_err: N`

O número de vezes que `ena_com_prepare_tx` apresentou falha para essa fila.

`queue_N_tx_bad_req_id: N`

`req_id` inválido para essa fila. O `req_id` válido é zero, menos `queue_size`, menos 1.

`queue_N_tx_llq_buffer_copy: N`

O número de pacotes cujo tamanho dos cabeçalhos é maior do que a entrada llq para essa fila.

`queue_N_tx_missed_tx: N`

O número de pacotes deixados sem conclusão para essa fila.

`queue_N_tx_unmask_interrupt: N`

O número de vezes que a interrupção tx foi desmascarada para essa fila.

`queue_N_rx_cnt: N`

O número de pacotes recebidos para essa fila.

`queue_N_rx_bytes: N`

O número de bytes recebidos para essa fila.

`queue_N_rx_rx_copybreak_pkt: N`

O número de vezes que a fila rx recebeu um pacote menor que o tamanho do pacote de rx\_copybreak para essa fila.

`queue_N_rx_csum_good: N`

O número de vezes que a fila rx recebeu um pacote em que a soma de verificação foi verificada e estava correta para essa fila.

`queue_N_rx_refil_partial: N`

O número de vezes que o driver não teve sucesso ao reabastecer a parte vazia da fila rx com buffers para essa fila. Se esse valor não for zero, isso indica recursos de memória baixa.

`queue_N_rx_bad_csum: N`

O número de vezes que a fila rx teve uma soma de verificação errada para a fila (somente se o descarregamento da soma de verificação for compatível).

`queue_N_rx_page_alloc_fail: N`

O número de vezes que a alocação de página apresentou falha para essa fila. Se esse valor não for zero, isso indica recursos de memória baixa.

`queue_N_rx_skb_alloc_fail: N`

O número de vezes que a alocação de SKB apresentou falha para essa fila. Se esse valor não for zero, isso indica recursos de sistema baixos.

`queue_N_rx_dma_mapping_err: N`

Contagem de erro de acesso da memória direta. Se esse valor não for 0, isso indica recursos de sistema baixos.

`queue_N_rx_bad_desc_num: N`

Excesso de buffers por pacote. Se o valor não for 0, isso indica o uso de buffers muito pequenos.

`queue_N_rx_bad_req_id: N`

O req\_id para essa fila não é válido. O req\_id válido é de [0, queue\_size - 1].

`queue_N_rx_empty_rx_ring: N`

O número de vezes que a fila rx estava vazia para essa fila.

`queue_N_rx_csum_unchecked: N`

O número de vezes que a fila rx recebeu um pacote cuja soma de verificação não foi verificada para essa fila.

`queue_N_rx_xdp_aborted: N`

O número de vezes que um pacote XDP foi classificado como XDP\_ABORT.

`queue_N_rx_xdp_drop: N`

O número de vezes que um pacote XDP foi classificado como XDP\_DROP.

`queue_N_rx_xdp_pass: N`

O número de vezes que um pacote XDP foi classificado como XDP\_PASS.

`queue_N_rx_xdp_tx: N`

O número de vezes que um pacote XDP foi classificado como XDP\_TX.

`queue_N_rx_xdp_invalid: N`

O número de vezes que o código de retorno XDP para o pacote não foi válido.

`queue_N_rx_xdp_redirect: N`

O número de vezes que um pacote XDP foi classificado como XDP\_REDIRECT.

`queue_N_xdp_tx_cnt: N`

O número de pacotes transmitidos para essa fila.

`queue_N_xdp_tx_bytes: N`

O número de bytes transmitidos para essa fila.

`queue_N_xdp_tx_queue_stop: N`

O número de vezes que essa fila estava cheia e interrompida.

`queue_N_xdp_tx_queue_wakeup: N`

O número de vezes que essa fila foi retomada depois de ser interrompida.

`queue_N_xdp_tx_dma_mapping_err: N`

Contagem de erro de acesso da memória direta. Se esse valor não for 0, isso indica recursos de sistema baixos.

`queue_N_xdp_tx_linearize: N`

O número de vezes que a linearização de buffer XDP foi tentada para essa fila.

`queue_N_xdp_tx_linearize_failed: N`

O número de vezes que a linearização do buffer XDP apresentou falha para essa fila.

`queue_N_xdp_tx_napi_comp: N`

O número de vezes que o manipulador napi chamou napi\_complete para essa fila.

`queue_N_xdp_tx_tx_poll: N`

O número de vezes que o manipulador napi foi programado para essa fila.

`queue_N_xdp_tx_doorbells: N`

O número de campainhas de transmissão para essa fila.

`queue_N_xdp_tx_prepare_ctx_err: N`

O número de vezes que ena\_com\_prepare\_tx apresentou falha para essa fila. Esse valor sempre deve ser zero; caso contrário, consulte os logs do driver.

`queue_N_xdp_tx_bad_req_id: N`

O req\_id para essa fila não é válido. O req\_id válido é de [0, queue\_size - 1].

`queue_N_xdp_tx_llq_buffer_copy: N`

O número de pacotes que tiveram seus cabeçalhos copiados usando a cópia do buffer llq para essa fila.

`queue_N_xdp_tx_missed_tx: N`

O número de vezes que uma entrada de fila tx perdeu um timeout de conclusão para essa fila.

`queue_N_xdp_tx_unmask_interrupt: N`

O número de vezes que a interrupção tx foi desmascarada para essa fila.

`ena_admin_q_aborted_cmd: N`

O número de comandos de administrador que foram abortados. Isso normalmente acontece durante o procedimento de autorrecuperação.

`ena_admin_q_submitted_cmd: N`

O número de campainhas da fila do administrador.

`ena_admin_q_completed_cmd: N`

O número de conclusões da fila do administrador.

`ena_admin_q_out_of_space: N`

O número de vezes que o driver tentou enviar o novo comando de administrador, mas a fila estava cheia.

`ena_admin_q_no_completion: N`

O número de vezes o driver não obteve a conclusão de um administrador para um comando.

## Logs de erro do driver no syslog

O driver do ENA grava mensagens de log para syslog durante a inicialização do sistema. Você pode examinar esses logs para procurar erros se estiver enfrentando problemas. Abaixo está um exemplo de informações registradas pelo driver do ENA no syslog durante a inicialização do sistema, junto com algumas anotações para mensagens selecionadas.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 478.416939] [ENA_COM: ena_com_validate_version]
ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 478.420915] [ENA_COM: ena_com_validate_version]
ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.256831] ena 0000:00:03.0: Device watchdog is
Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.672947] ena 0000:00:03.0: creating 8 io
queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.680885] [ENA_COM:
ena_com_init_interrupt_moderation] Feature 20 isn't supported // Interrupt moderation is
not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.691609] [ENA_COM: ena_com_get_feature_ex]
Feature 10 isn't supported // RSS HASH function configuration is not supported by the
device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.694583] [ENA_COM: ena_com_get_feature_ex]
Feature 18 isn't supported //RSS HASH input source configuration is not supported by the
device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.697433] [ENA_COM:
ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.701064] ena 0000:00:03.0 (unnamed
net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 479.704917] ena 0000:00:03.0: Elastic Network
Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:le:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 480.805037] EXT4-fs (xvdal): re-mounted. Opts:
(null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [ 481.025842] NET: Registered protocol family 10
```

Quais erros posso ignorar?

Os avisos a seguir que podem aparecer nos logs de erros do seu sistema podem ser ignorados para o Elastic Network Adapter:

Não há suporte para definição do atributo do host

Este dispositivo não oferece suporte aos atributos do host.

falha em alocar buffer para a fila rx

Esse é um erro recuperável e indica que pode ter havido um problema de pressão de memória quando o erro ocorreu.

Não há suporte para o recurso **X**

O recurso mencionado não é compatível com o Elastic Network Adapter. Os valores possíveis para **X** incluem:

- **10**: a configuração da função RSS Hash não é compatível para este dispositivo.
- **12**: a tabela RSS Indirection não é compatível para este dispositivo.
- **18**: a configuração de RSS Hash Input não é compatível para este dispositivo.
- **20**: a moderação de interrupção não é compatível para este dispositivo.
- **27**: o driver Elastic Network Adapter não oferece suporte à sondagem dos recursos de Ethernet de snmpd.

Falha ao configurar AENQ

O Elastic Network Adapter não oferece suporte à configuração de AENQ.

Tentativa de configurar eventos AENQ não compatíveis

Esse erro indica uma tentativa de configurar um grupo de eventos do AENQ que não são compatíveis com o Elastic Network Adapter.

## Elastic Fabric Adapter

O Elastic Fabric Adapter (EFA) é um dispositivo de rede que você pode anexar à instância do Amazon EC2 para acelerar as aplicações de machine learning e de Computação de Alta Performance (HPC). O EFA permite que você atinja a performance da aplicação de um cluster HPC no local, com a escalabilidade, a flexibilidade e a elasticidade fornecidas pela Nuvem AWS.

O EFA fornece latência mais baixa e mais consistente e maior rendimento que o transporte de TCP tradicionalmente usado em sistemas HPC baseados em nuvem. Ele aprimora a performance da comunicação entre instâncias, que é essencial para o dimensionamento de aplicações de machine learning e de HPC. Ele é otimizado para funcionar na infraestrutura de rede da AWS existente e pode ser dimensionado dependendo dos requisitos da aplicação.

O EFA se integra ao Libfabric 1.11.1 e oferece suporte a Open MPI 4.0.5 e Intel MPI Atualização 7 de 2019 para aplicações de HPC e a Nvidia Collective Communications Library (NCCL) para aplicações de machine learning.

### Note

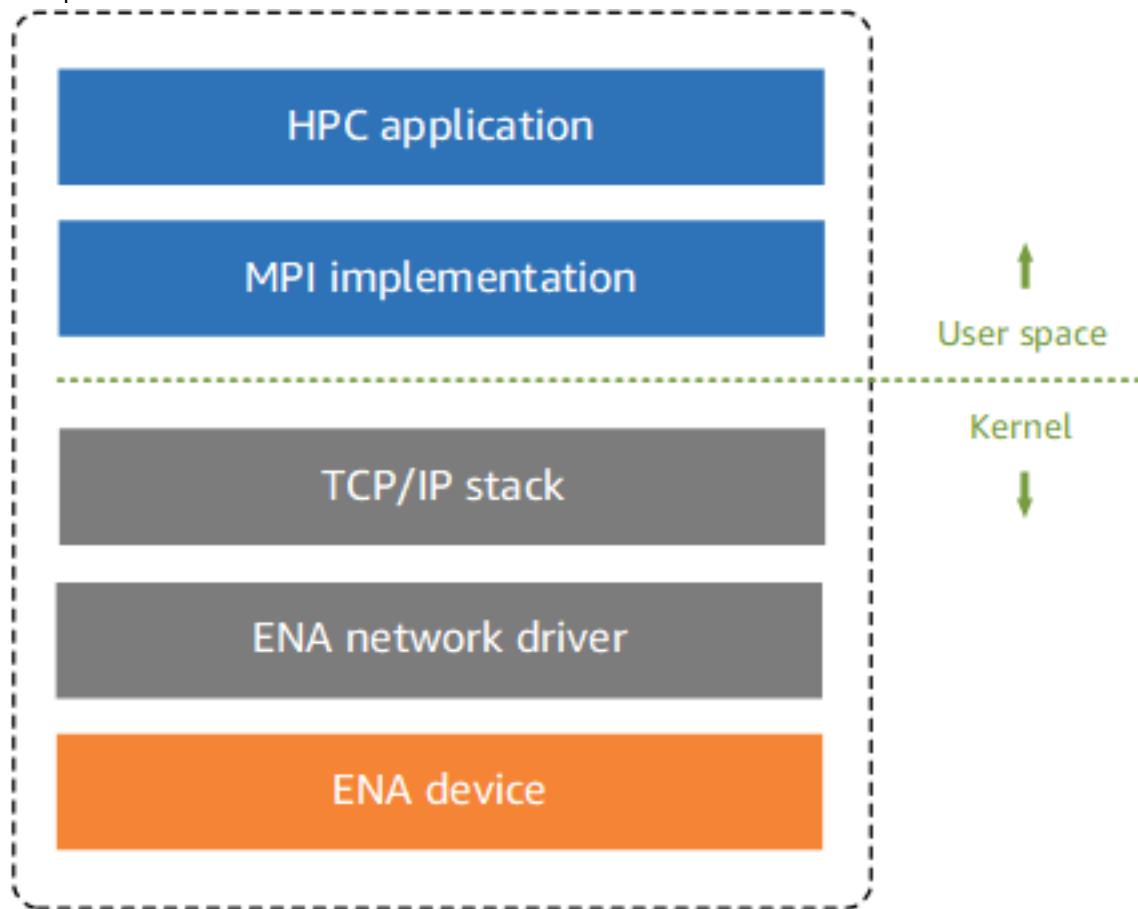
Os recursos de desvio de sistema operacional do EFAs não são compatíveis em instâncias do Windows. Se você anexar um EFA a uma instância do Windows, a instância funcionará como um Elastic Network Adapter, sem os recursos de EFA adicionais.

### Tópicos

- [Conceitos básicos de EFA \(p. 1045\)](#)
- [Interfaces e bibliotecas compatíveis \(p. 1046\)](#)
- [Tipos de instâncias compatíveis \(p. 1046\)](#)
- [AMIs compatíveis \(p. 1046\)](#)
- [Limitações de EFA \(p. 1047\)](#)
- [Conceitos básicos do EFA e MPI \(p. 1047\)](#)
- [Conceitos básicos do EFA e NCCL \(p. 1055\)](#)
- [Trabalhar com EFA \(p. 1078\)](#)
- [Monitorar um EFA \(p. 1081\)](#)
- [Verificar o instalador EFA usando uma soma de verificação \(p. 1082\)](#)

## Conceitos básicos de EFA

Um EFA é um Elastic Network Adapter (ENA) com recursos adicionais. Ele fornece todas as funcionalidades de um ENA, com uma funcionalidade adicional de desvio de sistema operacional. O desvio de sistema operacional é um modelo de acesso que permite que as aplicações de machine learning e de HPC se comuniquem diretamente com o hardware da interface de rede para fornecer funcionalidade de transporte confiável e de baixa latência.



### Traditional HPC software stack in EC2

Tradicionalmente, as aplicações HPC usam a Message Passing Interface (MPI) para fazer interface com o transporte de rede do sistema. Na Nuvem AWS, isso significa que as aplicações fazem interface com a MPI, que usa a pilha TCP/IP do sistema operacional e o driver de dispositivo ENA para habilitar a comunicação de rede entre as instâncias.

Com um EFA, aplicações HPC usam a MPI ou a NCCL para fazer interface com a API Libfabric. A API Libfabric ignora o kernel do sistema operacional e se comunica diretamente com o dispositivo EFA para colocar pacotes na rede. Isso reduz a sobrecarga e permite que a aplicação HPC seja executado com mais eficiência.

#### Note

O libfabric é um componente central do framework OpenFabrics Interfaces (OFI), que define e exporta a API do espaço do usuário do OFI. Para obter mais informações, consulte o site [Libfabric OpenFabrics](#).

## Diferenças entre EFAs e RIs

Elastic Network Adapters (ENAs) fornecem recursos tradicionais de rede IP que são necessários para permitir as redes da VPC. Os EFAs fornecem todos os mesmos recursos de rede IP tradicionais que os ENAs e também oferecem suporte a recursos de desvio do sistema operacional. O desvio de sistema operacional permite que as aplicações de machine learning e de HPC ignorem o kernel do sistema operacional e se comuniquem diretamente com o dispositivo EFA.

## Interfaces e bibliotecas compatíveis

O EFA oferece suporte às seguintes interfaces e bibliotecas:

- Open MPI 4.0.5
- Intel MPI 2019 Update 7
- NVIDIA Collective Communications Library (NCCL) 2.4.2 e posterior

## Tipos de instâncias compatíveis

Os tipos de instância a seguir são compatíveis com EFAs:

- Uso geral: m5dn.24xlarge | m5dn.metal | m5n.24xlarge | m5zn.12xlarge | m5zn.metal | m6i.32xlarge
- Otimizada para computação: c5n.18xlarge | c5n.metal | c6gn.16xlarge
- Otimizadas para memória: r5dn.24xlarge | r5dn.metal | r5n.24xlarge | r5n.metal
- Otimizadas para armazenamento: i3en.24xlarge | i3en.metal
- Computação acelerada: g4dn.metal | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge

Os tipos de instância disponíveis variam de acordo com a região. Para ver os tipos de instâncias disponíveis que oferecem suporte ao EFA em uma região, use o comando [describe-instance-types](#) com a opção --region e o código de região apropriado.

```
$ aws ec2 describe-instance-types \
--region us-east-2 \
--filters Name=network-info.efa-supported,Values=true \
--query "InstanceTypes[*].[InstanceType]" \
--output text
```

A seguir está um exemplo de saída.

```
g4dn.metal
i3en.24xlarge
r5n.24xlarge
c5n.18xlarge
m5n.24xlarge
inf1.24xlarge
m5dn.24xlarge
c5n.metal
p3dn.24xlarge
i3en.metal
r5dn.24xlarge
```

## AMIs compatíveis

Os AMIs a seguir oferecem suporte ao EFA com tipos de instância baseados em Intel x86:

- Amazon Linux 2
- CentOS 7 e 8
- RHEL 7 e 8
- Ubuntu 18.04 e 20.04
- SUSE Linux Enterprise 15 SP2
- openSUSE Leap 15.2 e posterior

Os AMIs a seguir oferecem suporte ao EFA com tipos de instância baseados em Arm (Graviton 2):

- Amazon Linux 2
- CentOS 8
- RHEL 8
- Ubuntu 18.04 e 20.04
- SUSE Linux Enterprise 15 SP2

## Limitações de EFA

O EFA tem as seguintes limitações:

- p4d.24xlargeAs instâncias oferecem suporte a até quatro EFAs. Todos os outros tipos de instância compatíveis oferecem suporte a apenas um EFA por instância.
- EFA O tráfego de desvio do sistema operacional é limitado a uma única sub-rede. Em outras palavras, o tráfego de EFA não pode ser enviado de uma sub-rede para outra. O tráfego IP normal do EFA pode ser enviado de uma sub-rede para outra.
- EFA O tráfego de desvio do sistema operacional não é roteável. O tráfego IP normal do EFA permanece roteável.
- O EFA deve ser um membro de um grupo de segurança que permita todo o tráfego de entrada e saída de e para o próprio grupo de segurança.
- O tráfego do EFA entre instâncias C6gn e outras instâncias habilitadas por EFA não é suportado.

## Conceitos básicos do EFA e MPI

Este tutorial ajuda a executar um cluster de instância habilitado para MPI e EFA para workloads de HPC. Neste tutorial, você seguirá as seguintes etapas:

### Tópicos

- [Etapa 1: Preparar um grupo de segurança habilitado para EFA \(p. 1048\)](#)
- [Etapa 2: Iniciar uma instância temporária \(p. 1048\)](#)
- [Etapa 3: Instalar o software EFA \(p. 1049\)](#)
- [Etapa 4: Desabilitar a proteção Ptrace \(p. 1051\)](#)
- [Etapa 5: \(Opcional\) Instalar o Intel MPI \(p. 1052\)](#)
- [Etapa 6: Instalar a aplicação HPC \(p. 1053\)](#)
- [Etapa 7: Criar uma AMI habilitada para EFA \(p. 1053\)](#)
- [Etapa 8: Iniciar instâncias habilitadas para EFA em um placement group de cluster \(p. 1053\)](#)
- [Etapa 9: Encerrar a instância temporária \(p. 1054\)](#)
- [Etapa 10: Habilitar SSH sem senha \(p. 1055\)](#)

## Etapa 1: Preparar um grupo de segurança habilitado para EFA

Um EFA requer um grupo de segurança que permita todo o tráfego de entrada e saída do grupo de segurança e para ele próprio. O procedimento a seguir permite todo o tráfego de entrada e saída apenas para fins de teste. Para outros cenários, consulte [Regras de grupo de segurança para diferentes casos de uso \(p. 1240\)](#).

Para criar um grupo de segurança habilitado para EFA

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, faça o seguinte:
  - a. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança, como EFA-enabled 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 executar suas instâncias habilitadas para EFA.
  - d. Escolha Create (Criar).
4. Selecione o grupo de segurança que você criou e, na guia Description (Descrição), copie o Group ID (ID do grupo).
5. Na guia Inbound (Entrada), faça o seguinte:
  - a. Selecione Edit.
  - b. Para Type (Tipo), escolha All traffic (Todo o tráfego).
  - c. Para Source (Origem), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
  - d. Escolha Save (Salvar).
6. Na guia Outbound (Saída), faça o seguinte:
  - a. Selecione Edit.
  - b. Para Type (Tipo), escolha All traffic (Todo o tráfego).
  - c. Para Destination (Destino), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
  - d. Escolha Save (Salvar).

## Etapa 2: Iniciar uma instância temporária

Execute uma instância temporária que você pode usar para instalar e configurar os componentes do software EFA. Você usa essa instância para criar um AMI habilitado para EFA a partir do qual você pode executar suas instâncias habilitadas para EFA.

Para executar uma instância temporária

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 AMI (Escolher uma AMI), escolha Select (Selecionar) para uma das [AMIs compatíveis \(p. 1046\)](#).
4. Na página Choose an Instance Type (Escolher um tipo de instância), selecione um dos [tipos de instância compatíveis \(p. 1046\)](#) e escolha Next: Configure Instance Details (Próximo: Configurar os detalhes da instância).

5. Na página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:
  - a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância.
  - b. Para Elastic Fabric Adapter, escolha Enable (Habilitar).
  - c. Na seção Network Interfaces (Interfaces de rede), para dispositivo eth0, escolha New network interface (Nova interface de rede).
  - d. Escolha Next: Add Storage.
6. Na página Add Storage (Adicionar armazenamento), especifique os volumes a serem anexados às instâncias, além dos volumes especificados pela AMI (como o volume do dispositivo raiz). Depois, selecione Next: Add Tags (Próximo: adicionar tags).
7. Na página Add Tags (Adicionar tags), especifique uma tag que você pode usar para identificar a instância temporária e escolha Next: Configure Security Group (Próximo: configurar grupo de segurança).
8. Na página Configure Security Group (Configurar grupo de segurança), para Assign a security group (Atribuir um grupo de segurança), selecione Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança que você criou na Etapa 1.
9. Na página Review Instance Launch (Revisar execução da instância), reveja as configurações e escolha Launch (Executar) para escolher um par de chaves e executar a instância.

## Etapa 3: Instalar o software EFA

Instale o kernel habilitado para EFA, drivers EFA, Libfabric e pilha Open MPI que é necessário para oferecer compatibilidade com EFA em sua instância temporária.

As etapas diferem dependendo de como você planeja usar o EFA com Open MPI, com Intel MPI ou com Open MPI e Intel MPI.

### Como instalar o software EFA

1. Conecte à instância que você iniciou. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. esse processo pode demorar alguns minutos.
  - Amazon Linux 2, RHEL 7/8 e CentOS 7/8

```
$ sudo yum update -y
```

- Ubuntu 18.04 e 20.04

```
$ sudo apt-get update
```

```
$ sudo apt-get upgrade -y
```

- SUSE Linux Enterprise

```
$ sudo zypper update -y
```

3. Faça download dos arquivos de instalação do software do EFA. Os arquivos de instalação do software são empacotados em um arquivo compactado tarball (.tar.gz). Para fazer download da última versão estável, use o seguinte comando:

```
$ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.13.0.tar.gz
```

Também é possível obter a versão mais recente substituindo o número da versão por `latest` no comando acima.

4. (Opcional) Verificar a autenticidade e a integridade do arquivo tarball do EFA (`.tar.gz`). Recomendamos que você faça isso para verificar a identidade do fornecedor do software e para verificar se a aplicação não foi alterada ou corrompida desde que foi publicada. Se você não deseja verificar o arquivo tarball, ignore esta etapa.

Note

Como alternativa, se preferir verificar o arquivo tarball usando uma soma de verificação MD5 ou SHA256, consulte [Verificar o instalador EFA usando uma soma de verificação \(p. 1082\)](#).

- a. Faça download da chave GPG pública e importe-a para seu pen-drive.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --import aws-efa-installer.key
```

O comando deve retornar um valor de chave. Anote o valor da chave, pois ele será necessário na próxima etapa.

- b. Verifique a impressão digital da chave GPG. Execute o seguinte comando e especifique o valor de chave da etapa anterior.

```
$ gpg --fingerprint key_value
```

O comando deve retornar uma impressão digital idêntica a `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC`. Se a impressão digital não corresponder, não execute o script de instalação do EFA e entre em contato com o AWS Support.

- c. Faça download do arquivo de assinatura e verifique a assinatura do arquivo tarball EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.13.0.tar.gz.sig && gpg --verify ./aws-efa-installer-1.13.0.tar.gz.sig
```

Veja a seguir um exemplo de saída.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:                 There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC
```

Se o resultado incluir `Good signature` e a impressão digital corresponda à impressão digital retornada na etapa anterior, vá para a próxima etapa. Se a impressão digital não corresponder, não execute o script de instalação do EFA e entre em contato com o AWS Support.

5. Extraia os arquivos do arquivo compactado `.tar.gz` e navegue para o diretório extraído.

```
$ tar -xf aws-efa-installer-1.13.0.tar.gz && cd aws-efa-installer
```

6. Instale o software EFA. Dependendo de seu caso de uso, faça o seguinte.

Note

Caso esteja usando um sistema operacional SUSE Linux, você deverá especificar também a opção `--skip-kmod` para impedir a instalação do kmod. Por padrão, o SUSE Linux não permite módulos fora da árvore do kernel. Como resultado, o suporte para EFA e NVIDIA GPUDirect atualmente não é compatível com o SUSE Linux.

- Open MPI e Intel MPI

Se planeja usar EFA com Open MPI e Intel MPI, você deve instalar o software EFA com Libfabric e Open MPI e concluir a Etapa 5: (Opcional) Instalar o Intel MPI. Para instalar o software EFA com Libfabric e Open MPI, execute o comando a seguir.

```
$ sudo ./efa_installer.sh -y
```

O Libfabric é instalado no diretório /opt/amazon/efa, enquanto a Open MPI é instalada no diretório /opt/amazon/openmpi.

- Somente Open MPI

Se planeja usar EFA com Open MPI, você deve instalar o software EFA com Libfabric e Open MPI e ignorar a Etapa 5: (Opcional) Instalar o Intel MPI. Para instalar o software EFA com Libfabric e Open MPI, execute o comando a seguir.

```
$ sudo ./efa_installer.sh -y
```

O Libfabric é instalado no diretório /opt/amazon/efa, enquanto a Open MPI é instalada no diretório /opt/amazon/openmpi.

- Somente Intel MPI

Se você pretende usar o EFA somente com Intel MPI, instale o software EFA sem Libfabric e Open MPI. Nesse caso, o Intel MPI usa o Libfabric incorporado. Se optar por fazer isso, você deve concluir a Etapa 5: (Opcional) Instalar o Intel MPI.

Para instalar o software EFA sem Libfabric e Open MPI, execute o comando a seguir.

```
$ sudo ./efa_installer.sh -y --minimal
```

7. Se o instalador do EFA solicitar que você reinicialize a instância, faça-o e, em seguida, reconecte-se à instância. Caso contrário, faça logout da instância e faça login novamente para concluir a instalação.
8. Confirme se os componentes do software EFA foram instalados com sucesso.

```
$ fi_info -p efa -t FI_EP_RDM
```

O comando deve retornar informações sobre as interfaces EFA Libfabric. O exemplo a seguir mostra a saída do comando.

```
provider: efa
    fabric: EFA-fe80::94:3dff:fe89:1b70
    domain: efa_0-rdm
    version: 2.0
    type: FI_EP_RDM
    protocol: FI_PROTO_EFA
```

## Etapa 4: Desabilitar a proteção Ptrace

Para melhorar a performance da aplicação HPC, o Libfabric usa a memória local da instância para comunicações entre processos quando os processos estão sendo executados na mesma instância.

O recurso de memória compartilhada usa CMA (Cross Memory Attach), que não é compatível com a proteção ptrace. Se estiver usando uma distribuição Linux que tenha a proteção ptrace habilitada por

padrão, como o Ubuntu, desabilite-a. Se a sua distribuição Linux não tiver a proteção ptrace habilitada por padrão, ignore esta etapa.

Como desabilitar a proteção ptrace

Execute um destes procedimentos:

- Para desabilitar temporariamente a proteção ptrace para fins de teste, execute o seguinte comando.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Para desabilitar permanentemente a proteção ptrace, adicione `kernel.yama.ptrace_scope = 0` a /etc/sysctl.d/10-ptrace.conf e reinicie a instância.

## Etapa 5: (Opcional) Instalar o Intel MPI

Important

Se você planejar usar apenas Open MPI, ignore esta etapa. Execute esta etapa se planejar usar a Intel MPI.

A Intel MPI exige uma instalação adicional e a configuração de uma variável de ambiente.

### Prerequisites

Verifique se o usuário que executa as etapas a seguir tem permissões de sudo.

Para instalar a Intel MPI

1. Para fazer download dos arquivos de instalação da Intel MPI, consulte o [site Intel Developer Zone](#).

Você deve se registrar para poder fazer download dos arquivos de configuração. Depois de registrar-se, faça o seguinte:

- a. Em Product (Produto), escolha Intel MPI Library for Linux.
  - b. Em Version (Versão), escolha Atualização 7 de 2019 e Full Product (Produto completo).
2. Os arquivos de instalação são empacotados em um arquivo compactado .tar.gz. Extraia os arquivos do arquivo compactado .tar.gz e navegue para o diretório extraído.

```
$ tar -xf file_name.tgz
```

```
$ cd directory_name
```

3. Abra o `silent.cfg` usando o editor de texto de sua preferência. Na linha 10, altere `ACCEPT_EULA=decline` para `ACCEPT_EULA=accept`. Salve as alterações e feche o arquivo.
4. Execute o script de instalação.

```
$ sudo ./install.sh -s silent.cfg
```

Por padrão, a Intel MPI é instalada no diretório /opt/intel/impi/.

5. Adicione as variáveis de ambiente da Intel MPI aos scripts de startup shell correspondentes para garantir que elas estejam definidas toda vez que a instância for iniciada. Dependendo de seu shell, faça o seguinte.
  - Para bash, adicione a seguinte variável de ambiente a `/home/username/.bashrc` e `/home/username/.bash_profile`.

```
source /opt/intel/compilers_and_libraries/linux/mpi/intel64/bin/mpivars.sh
```

- Para csh e tcsh, adicione a seguinte variável de ambiente a `/home/username/.cshrc`.

```
source /opt/intel/compilers_and_libraries/linux/mpi/intel64/bin/mpivars.csh
```

6. Saia da instância e faça login novamente.
7. Execute o comando a seguir para confirmar se a Intel MPI foi instalada com êxito.

```
$ which mpicc
```

Certifique-se de que o caminho retornado inclua o subdiretório `/opt/intel/`.

#### Note

Se você não usar mais a Intel MPI, remova as variáveis de ambiente dos scripts shell de startup.

## Etapa 6: Instalar a aplicação HPC

Instale a aplicação HPC na instância temporária. O procedimento de instalação varia dependendo da aplicação HPC específica. Para obter mais informações, consulte [Gerenciar software na instância do Amazon Linux \(p. 596\)](#).

#### Note

Pode ser necessário consultar a documentação da sua aplicação HPC para obter instruções de instalação.

## Etapa 7: Criar uma AMI habilitada para EFA

Depois de instalar os componentes de software necessários, crie uma AMI que possa ser reutilizada para executar suas instâncias habilitadas para o EFA.

Para criar uma AMI a partir de sua instância temporária

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), Image (Imagen), Create image (Criar imagem).
4. Em Create image (Criar imagem), faça o seguinte:
  - a. Em Image name (Nome da imagem), insira um nome descritivo para a AMI.
  - b. (Opcional) Em Image description (Descrição da imagem), informe a descrição do propósito da AMI.
  - c. Escolha Create Image (Criar imagem).
5. No painel de navegação, selecione AMIs.
6. Encontre a AMI que você criou na lista. Aguarde até que o status mude de pending para available antes de continuar para a próxima etapa.

## Etapa 8: Iniciar instâncias habilitadas para EFA em um placement group de cluster

Execute as instâncias habilitadas para EFA em um placement group de cluster usando a AMI habilitada para EFA criada na Etapa 7 e o grupo de segurança habilitado para EFA criado na Etapa 1.

### Note

Não é um requisito absoluto executar suas instâncias habilitadas para EFA em um placement group de cluster. No entanto, recomendamos a execução de suas instâncias habilitadas para EFA em um placement group de cluster ao executar as instâncias em um grupo de baixa latência em uma única zona de disponibilidade.

Para executar as instâncias habilitadas para EFA em um placement group de cluster.

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Launch Instance (Executar instância).
3. Na página Escolher uma AMI, selecione Minhas AMI, localize a AMI criada na Etapa 7 e selecione Escolher.
4. Na página Choose an Instance Type (Escolher um tipo de instância), selecione um dos [tipos de instância compatíveis \(p. 1046\)](#) e escolha Next: Configure Instance Details (Próximo: Configurar os detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:
  - a. Em Number of instances (Número de instâncias), insira o número de instâncias habilitadas para EFA que você deseja executar.
  - b. Em Network (Rede) e Subnet (Sub-rede), selecione a VPC e a sub-rede na qual executar as instâncias.
  - c. Em Placement group, selecione Add instance to placement group (Adicionar instância ao placement group).
  - d. Em Placement group name (Nome do placement group), selecione Add to a new placement group (Adicionar a um novo placement group), insira um nome descritivo para o placement group e para Placement group strategy (Estratégia de placement group), selecione cluster.
  - e. Para EFA, escolha Enable (Habilitar).
  - f. Na seção Network Interfaces (Interfaces de rede), para dispositivo eth0, escolha New network interface (Nova interface de rede). Como opção, você pode especificar um endereço IPv4 principal e um ou mais endereços IPv4 secundários. Se estiver executando a instância em uma sub-rede que tenha um bloco CIDR IPv6 associado, você poderá especificar opcionalmente um endereço IPv6 principal e um ou mais endereços IPv6 secundários.
  - g. Escolha Next: Add Storage.
6. Na página Add Storage (Adicionar armazenamento), especifique os volumes para anexar às instâncias em associação aos volumes especificados pela AMI (como o volume do dispositivo raiz) e escolha Next: Add Tags (Próximo: adicionar tags).
7. Na página Add Tags (Adicionar tags), especifique tags para as instâncias, como nome amigável, e selecione Next: Configure Security Group (Próximo: Configurar grupo de segurança).
8. Na página Configure Security Group (Configurar grupo de segurança), para Assign a security group (Atribuir um grupo de segurança), selecione Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança que você criou na Etapa 1.
9. Escolha Review and Launch.
10. Na página Review Instance Launch (Revisar execução da instância), reveja as configurações, e escolha Launch (Executar) para escolher um par de chaves e executar a instâncias.

## Etapa 9: Encerrar a instância temporária

Neste ponto, você não precisa mais da instância temporária que você executou. É possível encerrar a instância para não incorrer mais em cobranças desnecessárias.

Para encerrar a instância temporária

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 temporária, escolha Actions (Ações), selecione Instance state (Estado da instância), Terminate instance (Encerrar instance).
4. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

## Etapa 10: Habilitar SSH sem senha

Para permitir que suas aplicações sejam executadas em todas as instâncias do cluster, você deve habilitar o acesso SSH sem senha do nó líder para os nós membros. O nó líder é a instância a partir da qual você executa suas aplicações. As instâncias restantes no cluster são os nós membros.

Para habilitar SSH sem senha entre as instâncias no cluster

1. Selecione uma instância no cluster como o nó líder e conecte-se a ela.
2. Desabilite strictHostKeyChecking e habilite ForwardAgent no nó líder. Abra o `~/.ssh/config` usando o editor de texto de sua preferência e adicione o seguinte.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Gere um par de chaves RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

O par de chaves é criado no diretório do `$HOME/.ssh/`.

4. Altere as permissões da chave privada no nó líder.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Abra `~/.ssh/id_rsa.pub` usando seu editor de texto preferido e copie a chave.
6. Para cada nó de membro no cluster, faça o seguinte:
  - a. Conecte-se à instância.
  - b. Abra `~/.ssh/authorized_keys` usando o editor de texto de sua preferência e adicione a chave pública que você copiou anteriormente.
7. Para testar se o SSH sem senha está funcionando como esperado, conecte-se ao seu nó líder e execute o comando a seguir.

```
$ ssh member_node_private_ip
```

Você deve se conectar ao nó membro sem receber uma solicitação para inserir uma chave ou senha.

## Conceitos básicos do EFA e NCCL

A Nvidia Collective Communications Library (NCCL) é uma biblioteca de rotinas de comunicação coletiva padrão para várias GPUs em um único nó ou em vários nós. A NCCL pode ser usada com o EFA,

o Libfabric e a MPI para oferecer suporte a várias workloads de machine learning. Para obter mais informações, consulte o site da [NCCL](#).

Note

- A NCCL com o EFA só é compatível com as instâncias p3dn.24xlarge e p4d.24xlarge.
- Somente a NCCL 2.4.2 e posterior são compatíveis com EFA.

Os tutoriais a seguir ajudam a executar um cluster de instância habilitado para NCCL e EFA para workloads de machine learning.

- [Usar uma AMI de base \(p. 1056\)](#)
- [Usar uma AMI do AWS Deep Learning \(p. 1073\)](#)

## Usar uma AMI de base

As etapas a seguir ajudam você a começar a usar o Elastic Fabric Adapter uma das [AMIs de base compatíveis \(p. 1046\)](#).

Note

- Somente os tipos de instância p3dn.24xlarge e p4d.24xlarge são compatíveis.
- Somente AMIs básicas do Amazon Linux 2, RHEL 7/8, CentOS 7/8 e Ubuntu 18.04 são compatíveis.

### Tópicos

- [Etapa 1: Preparar um grupo de segurança habilitado para EFA \(p. 1056\)](#)
- [Etapa 2: Iniciar uma instância temporária \(p. 1057\)](#)
- [Etapa 3: Instalar drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN \(p. 1058\)](#)
- [Etapa 4: Instalar o software EFA \(p. 1066\)](#)
- [Etapa 5: Instalar a NCCL \(p. 1068\)](#)
- [Etapa 6: Instalar o plug-in aws-ofi-nccl \(p. 1068\)](#)
- [Etapa 7: Instalar os testes da NCCL \(p. 1069\)](#)
- [Etapa 8: Testar a configuração do EFA e da NCCL \(p. 1069\)](#)
- [Etapa 9: Instalar as aplicações de machine learning \(p. 1071\)](#)
- [Etapa 10: Criar um EFA e uma AMI habilitada para NCCL \(p. 1071\)](#)
- [Etapa 11: Encerrar a instância temporária \(p. 1071\)](#)
- [Etapa 12: Iniciar instâncias habilitadas para EFA e para NCCL em um placement group de cluster \(p. 1071\)](#)
- [Etapa 13: Habilitar SSH sem senha \(p. 1072\)](#)

### Etapa 1: Preparar um grupo de segurança habilitado para EFA

Um EFA requer um grupo de segurança que permita todo o tráfego de entrada e saída do grupo de segurança e para ele próprio. O procedimento a seguir permite todo o tráfego de entrada e saída apenas para fins de teste. Para outros cenários, consulte [Regras de grupo de segurança para diferentes casos de uso \(p. 1240\)](#).

Para criar um grupo de segurança habilitado para EFA

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, faça o seguinte:
  - a. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança, como EFA-enabled 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 executar suas instâncias habilitadas para EFA.
  - d. Escolha Create (Criar).
4. Selecione o grupo de segurança que você criou e, na guia Description (Descrição), copie o Group ID (ID do grupo).
5. Na guia Inbound (Entrada), faça o seguinte:
  - a. Selecione Edit.
  - b. Para Type (Tipo), escolha All traffic (Todo o tráfego).
  - c. Para Source (Origem), escolhaCustom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
  - d. Escolha Save (Salvar).
6. Na guia Outbound (Saída), faça o seguinte:
  - a. Selecione Edit.
  - b. Para Type (Tipo), escolha All traffic (Todo o tráfego).
  - c. Para Destination (Destino), escolhaCustom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
  - d. Escolha Save (Salvar).

## Etapa 2: Iniciar uma instância temporária

Execute uma instância temporária que você pode usar para instalar e configurar os componentes do software EFA. Você usa essa instância para criar um AMI habilitado para EFA a partir do qual você pode executar suas instâncias habilitadas para EFA.

### Para executar uma instância temporária

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 AMI (Escolher uma AMI), escolha uma das AMIs compatíveis.
4. Na página Choose an Instance Type (Escolher um tipo de instância), selecione p3dn.24xlarge ou p4d.24xlarge e selecione Next: Configure Instance Details (Próximo: configurar detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:
  - a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância.
  - b. Para Elastic Fabric Adapter, escolha Enable (Habilitar).
  - c. Na seção Network Interfaces (Interfaces de rede), para dispositivo eth0, escolha New network interface (Nova interface de rede).
  - d. Escolha Next: Add Storage.
6. Na página Add Storage (Adicionar armazenamento), especifique os volumes para anexar às instâncias, além dos volumes especificados pela AMI (como o volume do dispositivo raiz). Certifique-se de provisionar armazenamento suficiente para o toolkit Nvidia CUDA. Depois, selecione Next: Add Tags (Próximo: adicionar tags).

### Note

É necessário provisionar um armazenamento adicional de 10 a 20 GiB para o Toolkit Nvidia CUDA. Se você não provisionar armazenamento suficiente, você receberá uma mensagem de erro Espaço em disco insuficiente ao tentar instalar os drivers Nvidia e o Toolkit CUDA.

7. Na página Add Tags (Adicionar tags), especifique uma tag que você pode usar para identificar a instância temporária e escolha Next: Configure Security Group (Próximo: configurar grupo de segurança).
8. Na página Configure Security Group (Configurar grupo de segurança), em Assign a security group (Atribuir um grupo de segurança), escolha Select an existing security group (Escolher um grupo de segurança existente). Depois, selecione o grupo de segurança criado na Etapa 1.
9. Na página Review Instance Launch (Revisar execução da instância), reveja as configurações e escolha Launch (Executar) para escolher um par de chaves e executar a instância.

## Etapa 3: Instalar drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

Amazon Linux 2

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

1. Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

```
$ sudo yum groupinstall 'Development Tools' -y
```

2. Para usar o driver de GPU Nvidia, é necessário primeiro desabilitar os drivers de código aberto nouveau.
  - a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

- b. Adicione nouveau ao arquivo de lista de negação /etc/modprobe.d/blacklist.conf .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- c. Abra o /etc/default/grub usando o editor de texto de sua preferência e adicione o seguinte.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- d. Recompile a configuração do Grub.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

3. Reinicie a instância e reconecte-se a ela.
4. Instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.
  - a. Instale o repositório EPEL para DKMS e ative qualquer repositório opcional para sua distribuição Linux.

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- b. Instale a chave GPG pública do repositório CUDA.

```
$ distribution='rhel7'
```

- c. Configure o repositório de rede CUDA e atualize o cache do repositório.

```
$ ARCH=$( /bin/arch ) \  
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \  
&& sudo yum clean expire-cache
```

- d. Instale os drivers NVIDIA e CUDA e o cuDNN.

```
$ sudo yum clean all \  
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

5. Reinicialize a instância e reconecte-se a ela.  
6. (Somente instâncias p4d.24xlarge) Inicie o serviço Nvidia Fabric Manager e verifique se ele será iniciado automaticamente quando a instância for iniciada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager \  
&& sudo systemctl enable nvidia-fabricmanager
```

7. Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.
- Em shells bash, adicione as seguintes instruções a /home/*username*/.bashrc e /home/*username*/.bash\_profile.

```
export PATH=/usr/local/cuda/bin:$PATH  
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:  
$LD_LIBRARY_PATH
```

- Em shells tcsh, adicione as seguintes instruções a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH  
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:  
$LD_LIBRARY_PATH
```

8. Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

```
$ nvidia-smi -q | head
```

O comando deve retornar informações sobre os GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

CentOS 7/8

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

1. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância.

```
$ sudo yum upgrade -y && sudo reboot
```

Reconecte-se à sua instância depois de reinicializá-la.

2. Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

```
$ sudo yum groupinstall 'Development Tools' -y \  
&& sudo yum install -y tar bzip2 make automake pciutils elfutils-libelf-devel  
libglvnd-devel iptables firewalld vim bind-utils
```

3. Para usar o driver de GPU Nvidia, é necessário primeiro desabilitar os drivers de código aberto nouveau.
  - a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

- b. Adicione nouveau ao arquivo de lista de negação /etc/modprobe.d/blacklist.conf .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf  
blacklist vga16fb  
blacklist nouveau  
blacklist rivafb  
blacklist nvidiafb  
blacklist rivatv  
EOF
```

- c. Abra o /etc/default/grub usando o editor de texto de sua preferência e adicione o seguinte.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- d. Recompile a configuração do Grub.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Reinicie a instância e reconecte-se a ela.
5. Instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.

- a. Instale o repositório EPEL para DKMS e ative qualquer repositório opcional para sua distribuição Linux.

- CentOS 7

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- CentOS 8

```
$ sudo yum install -y epel-release
```

- b. Instale a chave GPG pública do repositório CUDA.

- CentOS 7

```
$ distribution='rhel7'
```

- CentOS 8

```
$ distribution='rhel8'
```

- Configure o repositório de rede CUDA e atualize o cache do repositório.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

- (Somente CentOS 8) Atualize o kernel em execução.

```
$ sudo yum install -y kernel kernel-core kernel-modules
```

- Instale os drivers NVIDIA e CUDA e o cuDNN.

```
$ sudo yum clean all \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

- Reinicialize a instância e reconecte-se a ela.

- (Somente instâncias p4d.24xlarge) Inicie o serviço Nvidia Fabric Manager e verifique se ele será iniciado automaticamente quando a instância for iniciada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager \
&& sudo systemctl enable nvidia-fabricmanager
```

- Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.

- Em shells bash, adicione as seguintes instruções a /home/*username*/.bashrc e /home/*username*/.bash\_profile.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:
$LD_LIBRARY_PATH
```

- Em shells tcsh, adicione as seguintes instruções a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:
$LD_LIBRARY_PATH
```

- Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

```
$ nvidia-smi -q | head
```

O comando deve retornar informações sobre os GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

## RHEL 7/8

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

- Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

```
$ sudo yum groupinstall 'Development Tools' -y
```

2. Para usar o driver de GPU Nvidia, é necessário primeiro desabilitar os drivers de código aberto nouveau.
  - a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

- b. Adicione nouveau ao arquivo de lista de negação /etc/modprobe.d/blacklist.conf .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- c. Abra o /etc/default/grub usando o editor de texto de sua preferência e adicione o seguinte.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- d. Recompile a configuração do Grub.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

3. Reinicie a instância e reconecte-se a ela.
4. Instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.

- a. Instale o repositório EPEL para DKMS e ative qualquer repositório opcional para sua distribuição Linux.

- RHEL 7

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- RHEL 8

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

- b. Instale a chave GPG pública do repositório CUDA.

```
$ distribution=$( . /etc/os-release;echo $ID`rpm -E "%{?rhel} %{?fedora}"` )
```

- c. Configure o repositório de rede CUDA e atualize o cache do repositório.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

- d. Instale os drivers NVIDIA e CUDA e o cuDNN.

```
$ sudo yum clean all \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

5. Reinicialize a instância e reconecte-se a ela.
6. (Somente instâncias p4d.24xlarge) Inicie o serviço Nvidia Fabric Manager e verifique se ele será iniciado automaticamente quando a instância for iniciada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager \
&& sudo systemctl enable nvidia-fabricmanager
```

7. Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.
  - Em shells bash, adicione as seguintes instruções a /home/*username*/ .bashrc e /home/*username*/ .bash\_profile.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:
$LD_LIBRARY_PATH
```

- Em shells tcsh, adicione as seguintes instruções a /home/*username*/ .cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:
$LD_LIBRARY_PATH
```

8. Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

```
$ nvidia-smi -q | head
```

O comando deve retornar informações sobre os GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

Ubuntu 18.04/20.04

Para instalar os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN

1. Instale os utilitários necessários para instalar os drivers de GPU Nvidia e o toolkit Nvidia CUDA.

```
$ sudo apt-get update \
&& sudo apt-get install build-essential -y
```

2. Para usar o driver de GPU Nvidia, é necessário primeiro desabilitar os drivers de código aberto nouveau.
  - a. Instale os utilitários necessários e o pacote de cabeçalhos kernel para a versão do kernel que está sendo executada.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

- b. Adicione nouveau ao arquivo de lista de negação /etc/modprobe.d/blacklist.conf .

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
```

```
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

- c. Abra o /etc/default/grub usando o editor de texto de sua preferência e adicione o seguinte.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

- d. Recompile a configuração do Grub.

```
$ sudo update-grub
```

3. Reinicialize a instância e reconecte-se a ela.  
4. Instale os drivers de GPU Nvidia, o toolkit Nvidia CUDA e o cuDNN.  
a. Faça download e instale as dependências adicionais e adicione o repositório CUDA.

- Ubuntu 18.04

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu1804/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu1804/x86_64/nvidia-machine-learning-repo-
ubuntu1804_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu1804/x86_64/cuda-ubuntu1804.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu1804/x86_64/7fa2af80.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu1804/x86_64/ /' \
&& sudo apt update
```

- Ubuntu 20.04

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update
```

- b. Instale os drivers NVIDIA e CUDA e o cuDNN.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers cuda-
toolkit-11-0 libcudnn8 libcu-dnn8-dev -y
```

5. Reinicialize a instância e reconecte-se a ela.  
6. (p4d.24xlarge somente instâncias) Instale o Nvidia Fabric Manager.

- a. Você deve instalar a versão do Nvidia Fabric Manager que corresponde à versão do módulo do kernel Nvidia que você instalou na etapa anterior.

Execute o seguinte comando para determinar a versão do módulo do kernel Nvidia.

```
$ cat /proc/driver/nvidia/version | grep "Kernel Module"
```

A seguir está um exemplo de saída.

```
NVRM version: NVIDIA UNIX x86_64 Kernel Module 450.42.01 Tue Jun 15 21:26:37  
UTC 2021
```

No exemplo acima, a versão principal 450 do módulo do kernel foi instalado. Isso significa que você precisa instalar a versão do Nvidia Fabric Manager 450.

- b. Instale o Nvidia Fabric Manager. Execute o seguinte comando e especifique a versão principal identificada na etapa anterior.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-fabricmanager-  
major_version_number
```

Por exemplo, se a versão principal 450 do módulo do kernel foi instalado, use o seguinte comando para instalar a versão correspondente do Nvidia Fabric Manager.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-fabricmanager-450
```

- c. Inicie o serviço e certifique-se de que ele seja iniciado automaticamente quando a instância for executada. O Nvidia Fabric Manager é necessário para o gerenciamento do NV Switch.

```
$ sudo systemctl start nvidia-fabricmanager \  
&& sudo systemctl enable nvidia-fabricmanager
```

7. Certifique-se de que os caminhos do CUDA sejam definidos cada vez que a instância for executada.

- Em shells bash, adicione as seguintes instruções a /home/*username*/.bashrc e /home/*username*/.bash\_profile.

```
export PATH=/usr/local/cuda/bin:$PATH  
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:  
$LD_LIBRARY_PATH
```

- Em shells tcsh, adicione as seguintes instruções a /home/*username*/.cshrc.

```
setenv PATH=/usr/local/cuda/bin:$PATH  
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/lib64:  
$LD_LIBRARY_PATH
```

8. Para verificar se os drivers de GPU Nvidia estão funcionando, execute o comando a seguir.

```
$ nvidia-smi -q | head
```

O comando deve retornar informações sobre os GPUs Nvidia, sobre os drivers de GPU Nvidia e sobre o toolkit Nvidia CUDA.

## Etapa 4: Instalar o software EFA

Instale o kernel habilitado para EFA, drivers EFA, Libfabric e pilha Open MPI que é necessário para oferecer compatibilidade com EFA em sua instância temporária.

### Como instalar o software EFA

1. Conecte à instância que você iniciou. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. Para garantir que todos os pacotes de software estejam atualizados, execute uma atualização rápida de software em sua instância. esse processo pode demorar alguns minutos.
  - Amazon Linux 2, RHEL 7/8 e CentOS 7/8

```
$ sudo yum update -y
```

- Ubuntu 18.04

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

3. Faça download dos arquivos de instalação do software do EFA. Os arquivos de instalação do software são empacotados em um arquivo compactado tarball (.tar.gz). Para fazer download da última versão estável, use o seguinte comando:

```
$ curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.13.0.tar.gz
```

Também é possível obter a versão mais recente substituindo o número da versão por latest no comando acima.

4. (Opcional) Verificar a autenticidade e a integridade do arquivo tarball do EFA (.tar.gz). Recomendamos que você faça isso para verificar a identidade do fornecedor do software e para verificar se a aplicação não foi alterada ou corrompida desde que foi publicada. Se você não deseja verificar o arquivo tarball, ignore esta etapa.

### Note

Como alternativa, se preferir verificar o arquivo tarball usando uma soma de verificação MD5 ou SHA256, consulte [Verificar o instalador EFA usando uma soma de verificação \(p. 1082\)](#).

- a. Faça download da chave GPG pública e importe-a para seu pen-drive.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --import aws-efa-installer.key
```

O comando deve retornar um valor de chave. Anote o valor da chave, pois ele será necessário na próxima etapa.

- b. Verifique a impressão digital da chave GPG. Execute o seguinte comando e especifique o valor de chave da etapa anterior.

```
$ gpg --fingerprint key_value
```

O comando deve retornar uma impressão digital idêntica a 4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC. Se a impressão digital não corresponder, não execute o script de instalação do EFA e entre em contato com o AWS Support.

- c. Faça download do arquivo de assinatura e verifique a assinatura do arquivo tarball EFA.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.13.0.tar.gz.sig &&  
gpg --verify ./aws-efa-installer-1.13.0.tar.gz.sig
```

Veja a seguir um exemplo de saída.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC  
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"  
gpg: WARNING: This key is not certified with a trusted signature!  
gpg:                 There is no indication that the signature belongs to the owner.  
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC
```

Se o resultado incluir **Good signature** e a impressão digital corresponda à impressão digital retornada na etapa anterior, vá para a próxima etapa. Se a impressão digital não corresponder, não execute o script de instalação do EFA e entre em contato com o AWS Support.

5. Extraia os arquivos do arquivo compactado `.tar.gz` e navegue para o diretório extraído.

```
$ tar -xf aws-efa-installer-1.13.0.tar.gz && cd aws-efa-installer
```

6. Execute o script de instalação do software EFA.

```
$ sudo ./efa_installer.sh -y -g
```

O Libfabric é instalado no diretório `/opt/amazon/efa`, enquanto a Open MPI é instalada no diretório `/opt/amazon/openmpi`.

7. Se o instalador do EFA solicitar que você reinicialize a instância, faça-o e, em seguida, reconecte-se à instância. Caso contrário, faça logout da instância e faça login novamente para concluir a instalação.
8. Confirme se os componentes do software EFA foram instalados com sucesso.

```
$ fi_info -p efa -t FI_EP_RDM
```

O comando deve retornar informações sobre as interfaces EFA Libfabric. O exemplo a seguir mostra a saída do comando.

- p3dn.24xlarge com interface de rede única

```
provider: efa  
fabric: EFA-fe80::94:3dff:fe89:1b70  
domain: efa_0-rdm  
version: 2.0  
type: FI_EP_RDM  
protocol: FI_PROTO_EFA
```

- p4d.24xlarge com várias interfaces de rede

```
provider: efa  
fabric: EFA-fe80::c6e:8fff:fef6:e7ff  
domain: efa_0-rdm  
version: 111.0  
type: FI_EP_RDM  
protocol: FI_PROTO_EFA  
provider: efa  
fabric: EFA-fe80::c34:3eff:feb2:3c35  
domain: efa_1-rdm  
version: 111.0  
type: FI_EP_RDM
```

```
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

## Etapa 5: Instalar a NCCL

Instale a NCCL. Para obter mais informações sobre a NCCL, consulte o [Repositório da NCCL](#).

### Como instalar a NCCL

1. Navegue até o diretório /opt.

```
$ cd /opt
```

2. Clone o repositório oficial da NCCL para a instância e navegue até o repositório local clonado.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git && cd nccl
```

3. Compile e instale a NCCL e especifique o diretório de instalação do CUDA.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

## Etapa 6: Instalar o plug-in aws-ofi-nccl

O plug-in aws-ofi-nccl mapeia as APIs de transporte orientadas para a conexão da NCCL para a interface de conexão menos confiável do Libfabric. Isso permite usar o Libfabric como um provedor de rede ao executar aplicações baseadas na NCCL. Para obter mais informações sobre o plug-in aws-ofi-nccl, consulte o [Repositório do aws-ofi-nccl](#).

### Como instalar o plug-in aws-ofi-nccl

1. Navegue até o diretório inicial.

```
$ cd $HOME
```

2. (Somente Ubuntu) Instale os utilitários necessários para instalar o plug-in aws-ofi-nccl. Para instalar os utilitários exigidos, execute o comando a seguir.

```
$ sudo apt-get install libtool autoconf -y
```

3. Clone a ramificação aws do repositório oficial aws-ofi-nccl da AWS para a instância e navegue até o repositório local clonado.

```
$ git clone https://github.com/aws/aws-ofi-nccl.git -b aws && cd aws-ofi-nccl
```

4. Para gerar o script `configure`, execute o script `autogen.sh`.

```
$ ./autogen.sh
```

5. Para gerar os arquivos make, execute o script `configure` e especifique os diretórios de instalação da MPI, do Libfabric, da NCCL e do CUDA.

```
$ ./configure --prefix=/opt/aws-ofi-nccl --with-mpi=/opt/amazon/openmpi \  
--with-libfabric=/opt/amazon/efa --with-nccl=/opt/nccl/build \  
--with-cuda=/usr/local/cuda
```

6. Adicione o diretório Open MPI à variável `PATH`.

```
$ export PATH=/opt/amazon/openmpi/bin/:$PATH
```

7. Instale o plug-in aws-ofi-nccl.

```
$ make \  
&& sudo make install
```

## Etapa 7: Instalar os testes da NCCL

Instale os testes da NCCL. Os testes da NCCL permitem confirmar se a NCCL está instalada adequadamente se ela está funcionando conforme esperado. Para obter mais informações sobre os testes da NCCL, consulte o [Repositório nccl-tests](#).

### Como instalar os testes da NCCL

1. Navegue até o diretório inicial.

```
$ cd $HOME
```

2. Clone o repositório oficial de nccl-tests para a instância e navegue até o repositório local clonado.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Adicione o diretório do Libfabric à variável `LD_LIBRARY_PATH`.

- Amazon Linux, Amazon Linux 2, RHEL e CentOS

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
```

- Ubuntu 18.04

```
$ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
```

4. Instale os testes da NCCL e especifique os diretórios de instalação da MPI da NCCL e do CUDA.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/local/cuda
```

## Etapa 8: Testar a configuração do EFA e da NCCL

Execute um teste para verificar se a instância temporária está configurada adequadamente para o EFA e para a NCCL.

## Como testar a configuração do EFA e da NCCL

- Crie um arquivo de host que especifique os hosts nos quais executar os testes. O comando a seguir cria um arquivo de host chamado `my-hosts` que inclui uma referência à própria instância.

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/local-ipv4 >> my-hosts
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-hosts
```

- Execute o teste e especifique o arquivo de host (`--hostfile`) e o número de GPUs a serem usadas (`-n`). O comando a seguir executa o teste `all_reduce_perf` em 8 GPUs na própria instância e especifica as variáveis de ambiente a seguir.

- `FI_PROVIDER="efa"`: especifica o provedor da interface do fabric. Isso deve ser definido como "efa".
- `FI_EFA_USE_DEVICE_RDMA=1`: usa a funcionalidade RDMA do dispositivo para transferência unilateral e bilateral.
- `NCCL_DEBUG=INFO`: habilita a saída de depuração detalhada. Também é possível especificar `VERSION` para imprimir somente a versão da NCCL no início do teste ou `WARN` para receber somente mensagens de erro.
- `NCCL_ALGO=ring`: habilita o algoritmo em anel para operações coletivas.

Para obter mais informações sobre os argumentos de teste da NCCL, consulte o [README NCCL Tests](#) no repositório oficial de nccl-tests.

```
$ /opt/amazon/openmpi/bin/mpirun \
-x FI_PROVIDER="efa" \
-x FI_EFA_USE_DEVICE_RDMA=1 \
-x RDMAV_FORK_SAFE=1 \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib64:/opt/amazon/openmpi/lib64:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
-x NCCL_ALGO=ring \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to none \
$HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- Você pode confirmar se EFA está ativo como o provedor subjacente para NCCL quando o log `NCCL_DEBUG` é impresso.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

As seguintes informações adicionais são exibidas ao usar uma instância `p4d.24xlarge`.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-ofi-
nccl/xml/p4d-24x1-topo.xml
```

## Etapa 9: Instalar as aplicações de machine learning

Instale as aplicações de machine learning na instância temporária. O procedimento de instalação varia dependendo da aplicação de machine learning específica. Para obter mais informações sobre como instalar software em sua instância do Linux, consulte [Gerenciamento de software em sua instância do Linux](#).

### Note

Pode ser necessário consultar a documentação da sua aplicação de machine learning para obter instruções de instalação.

## Etapa 10: Criar um EFA e uma AMI habilitada para NCCL

Depois de instalar os componentes de software necessários, crie uma AMI que possa ser reutilizada para executar suas instâncias habilitadas para o EFA.

Para criar uma AMI a partir de sua instância temporária

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), Image (Imagen), Create image (Criar imagem).
4. Em Create image (Criar imagem), faça o seguinte:
  - a. Em Image name (Nome da imagem), insira um nome descritivo para a AMI.
  - b. (Opcional) Em Image description (Descrição da imagem), informe a descrição do propósito da AMI.
  - c. Escolha Create Image (Criar imagem).
5. No painel de navegação, selecione AMIs.
6. Encontre a AMI que você criou na lista. Aguarde até que o status mude de pending para available antes de continuar para a próxima etapa.

## Etapa 11: Encerrar a instância temporária

Neste ponto, você não precisa mais da instância temporária que você executou. É possível encerrar a instância para não incorrer mais em cobranças desnecessárias.

Para encerrar a instância temporária

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 temporária, escolha Actions (Ações), selecione Instance state (Estado da instância), Terminate instance (Encerrar instance).
4. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

## Etapa 12: Iniciar instâncias habilitadas para EFA e para NCCL em um placement group de cluster

Execute as instâncias habilitadas para EFA em um grupo de posicionamento de cluster usando a AMI habilitada para EFA criada e o grupo de segurança habilitado para EFA criado anteriormente.

Para executar as instâncias habilitadas para EFA e NCCL em um grupo de posicionamento de cluster.

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 AMI (Escolher uma AMI), selecione My AMIs (Minhas AMIs), localize a AMI criada anteriormente e escolha Select (Selecionar).
4. Na página Choose an Instance Type (Escolher um tipo de instância), escolha p3dn.24xlarge e selecione Next: Configure Instance Details (Próximo: configurar detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:
  - a. Em Number of instances (Número de instâncias), insira o número de instâncias habilitadas para EFA e NCCL que você deseja executar.
  - b. Em Network (Rede) e Subnet (Sub-rede), selecione a VPC e a sub-rede na qual executar as instâncias.
  - c. Em Placement group, selecione Add instance to placement group (Adicionar instância ao placement group).
  - d. Em Placement group name (Nome do grupo de posicionamento), selecione Add to a new placement group (Adicionar a um novo grupo de posicionamento) e, em seguida, insira um nome descritivo para o grupo de posicionamento. Em seguida, em Placement group strategy (Estratégia do grupo de posicionamento), selecione cluster.
  - e. Para EFA, escolha Enable (Habilitar).
  - f. Na seção Network Interfaces (Interfaces de rede), para dispositivo eth0, escolha New network interface (Nova interface de rede). Como opção, você pode especificar um endereço IPv4 principal e um ou mais endereços IPv4 secundários. Se estiver executando a instância em uma sub-rede que tenha um bloco CIDR IPv6 associado, você poderá especificar opcionalmente um endereço IPv6 principal e um ou mais endereços IPv6 secundários.
  - g. Escolha Next: Add Storage.
6. Na página Add Storage (Adicionar armazenamento), especifique os volumes para anexar às instâncias, além dos volumes especificados pela AMI (como o volume raiz). Depois, selecione Next: Add Tags (Próximo: adicionar tags).
7. Na página Add Tags (Adicionar tags), especifique tags para as instâncias, como nome amigável, e selecione Next: Configure Security Group (Próximo: Configurar grupo de segurança).
8. Na página Configure Security Group (Configurar grupo de segurança), para Assign a security group (Atribuir um grupo de segurança), selecione Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança que você criou anteriormente.
9. Escolha Review and Launch.
10. Na página Review Instance Launch (Revisar execução da instância), reveja as configurações, e escolha Launch (Executar) para escolher um par de chaves e executar a instâncias.

## Etapa 13: Habilitar SSH sem senha

Para permitir que suas aplicações sejam executadas em todas as instâncias do cluster, você deve habilitar o acesso SSH sem senha do nó líder para os nós membros. O nó líder é a instância a partir da qual você executa suas aplicações. As instâncias restantes no cluster são os nós membros.

Para habilitar SSH sem senha entre as instâncias no cluster

1. Selecione uma instância no cluster como o nó líder e conecte-se a ela.
2. Desabilite strictHostKeyChecking e habilite ForwardAgent no nó líder. Abra o `~/.ssh/config` usando o editor de texto de sua preferência e adicione o seguinte.

```
Host *
  ForwardAgent yes
Host *
  StrictHostKeyChecking no
```

3. Gere um par de chaves RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

O par de chaves é criado no diretório do `$HOME/.ssh/`.

4. Altere as permissões da chave privada no nó líder.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Abra `~/.ssh/id_rsa.pub` usando seu editor de texto preferido e copie a chave.
6. Para cada nó de membro no cluster, faça o seguinte:
  - a. Conecte-se à instância.
  - b. Abra `~/.ssh/authorized_keys` usando o editor de texto de sua preferência e adicione a chave pública que você copiou anteriormente.
7. Para testar se o SSH sem senha está funcionando como esperado, conecte-se ao seu nó líder e execute o comando a seguir.

```
$ ssh member_node_private_ip
```

Você deve se conectar ao nó membro sem receber uma solicitação para inserir uma chave ou senha.

## Usar uma AMI do AWS Deep Learning

As etapas a seguir ajudam a começar a usar uma das seguintes AMIs do AWS Deep Learning:

- AMI do Deep Learning (Amazon Linux 2) versão 25.0 e posterior
- AMI do Deep Learning (Amazon Linux) versão 25.0 e posterior
- AMI do Deep Learning (Ubuntu 18.04) versão 25.0 e posterior
- AMI do Deep Learning (Ubuntu 16.04) versão 25.0 e posterior

Para obter mais informações, consulte o [Guia do usuário do AWS Deep Learning AMI](#).

### Note

Somente os tipos de instância `p3dn.24xlarge` e `p4d.24xlarge` são compatíveis.

### Tópicos

- [Etapa 1: Preparar um grupo de segurança habilitado para EFA \(p. 1074\)](#)
- [Etapa 2: Iniciar uma instância temporária \(p. 1074\)](#)
- [Etapa 3: Testar a configuração do EFA e da NCCL \(p. 1075\)](#)
- [Etapa 4: Instalar as aplicações de machine learning \(p. 1076\)](#)
- [Etapa 5: Criar um EFA e uma AMI habilitada para NCCL \(p. 1076\)](#)
- [Etapa 6: Encerrar a instância temporária \(p. 1077\)](#)
- [Etapa 7: Iniciar instâncias habilitadas para o EFA e para a NCCL em um placement group de cluster \(p. 1077\)](#)
- [Etapa 8: Habilitar SSH sem senha \(p. 1078\)](#)

## Etapa 1: Preparar um grupo de segurança habilitado para EFA

Um EFA requer um grupo de segurança que permita todo o tráfego de entrada e saída do grupo de segurança e para ele próprio. O procedimento a seguir permite todo o tráfego de entrada e saída apenas para fins de teste. Para outros cenários, consulte [Regras de grupo de segurança para diferentes casos de uso \(p. 1240\)](#).

Para criar um grupo de segurança habilitado para EFA

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, faça o seguinte:
  - a. Em Security group name (Nome do grupo de segurança), insira um nome descritivo para o grupo de segurança, como **EFA-enabled 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 executar suas instâncias habilitadas para EFA.
  - d. Escolha Create (Criar).
4. Selecione o grupo de segurança que você criou e, na guia Description (Descrição), copie o Group ID (ID do grupo).
5. Na guia Inbound (Entrada), faça o seguinte:
  - a. Selecione Edit.
  - b. Para Type (Tipo), escolha All traffic (Todo o tráfego).
  - c. Para Source (Origem), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
  - d. Escolha Save (Salvar).
6. Na guia Outbound (Saída), faça o seguinte:
  - a. Selecione Edit.
  - b. Para Type (Tipo), escolha All traffic (Todo o tráfego).
  - c. Para Destination (Destino), escolha Custom (Personalizado) e cole o ID do grupo de segurança que você copiou no campo.
  - d. Escolha Save (Salvar).

## Etapa 2: Iniciar uma instância temporária

Execute uma instância temporária que você pode usar para instalar e configurar os componentes do software EFA. Você usa essa instância para criar um AMI habilitado para EFA a partir do qual você pode executar suas instâncias habilitadas para EFA.

Para executar uma instância temporária

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 AMI (Escolher uma AMI), escolha uma AMI do AWS Deep Learning versão 25.0 ou posterior.
4. Na página Choose an Instance Type (Escolher um tipo de instância), selecione **p3dn.24xlarge** ou **p4d.24xlarge** e selecione Next: Configure Instance Details (Próximo: configurar detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:

- a. Em Subnet (Sub-rede), escolha a sub-rede na qual deseja iniciar a instância.
- b. Para Elastic Fabric Adapter, escolha Enable (Habilitar).
- c. Na seção Network Interfaces (Interfaces de rede), para dispositivo eth0, escolha New network interface (Nova interface de rede).
- d. Escolha Next: Add Storage.
6. Na página Add Storage (Adicionar armazenamento), especifique os volumes para anexar às instâncias, além dos volumes especificados pela AMI (como o volume do dispositivo raiz). Depois, selecione Next: Add Tags (Próximo: adicionar tags).
7. Na página Add Tags (Adicionar tags), especifique uma tag que você pode usar para identificar a instância temporária e escolha Next: Configure Security Group (Próximo: configurar grupo de segurança).
8. Na página Configure Security Group (Configurar grupo de segurança), em Assign a security group (Atribuir um grupo de segurança), escolha Select an existing security group (Escolher um grupo de segurança existente). Depois, selecione o grupo de segurança criado na Etapa 1.
9. Na página Review Instance Launch (Revisar execução da instância), reveja as configurações e escolha Launch (Executar) para escolher um par de chaves e executar a instância.

### Etapa 3: Testar a configuração do EFA e da NCCL

Execute um teste para verificar se a instância temporária está configurada adequadamente para o EFA e para a NCCL.

#### Como testar a configuração do EFA e da NCCL

1. Crie um arquivo de host que especifique os hosts nos quais executar os testes. O comando a seguir cria um arquivo de host chamado my-hosts que inclui uma referência à própria instância.

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/local-ipv4 >> my-hosts
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-hosts
```

2. Execute o teste e especifique o arquivo de host (--hostfile) e o número de GPUs a serem usadas (-n). O comando a seguir executa o teste all\_reduce\_perf em 8 GPUs na própria instância e especifica as variáveis de ambiente a seguir.
  - **FI\_PROVIDER="efa"**: especifica o provedor da interface do fabric. Isso deve ser definido como "efa".
  - **FI\_EFA\_USE\_DEVICE\_RDMA=1**: usa a funcionalidade RDMA do dispositivo para transferência unilateral e bilateral.
  - **NCCL\_DEBUG=INFO**: habilita a saída de depuração detalhada. Também é possível especificar **VERSION** para imprimir somente a versão da NCCL no início do teste ou **WARN** para receber somente mensagens de erro.
  - **NCCL\_ALGO=ring**: habilita o algoritmo em anel para operações coletivas.

Para obter mais informações sobre os argumentos de teste da NCCL, consulte o [README NCCL Tests](#) no repositório oficial de nccl-tests.

```
$ /opt/amazon/openmpi/bin/mpirun \
-x FI_PROVIDER="efa" \
-x FI_EFA_USE_DEVICE_RDMA=1 \
-x RDMAV_FORK_SAFE=1 \
-x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib64:/opt/amazon/openmpi/lib64:/usr/local/cuda/efa/lib:$LD_LIBRARY_PATH \
-x NCCL_DEBUG=INFO \
-x NCCL_ALGO=ring \
--hostfile my-hosts -n 8 -N 8 \
--mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-to none
\ \
$HOME/src/bin/efa-tests/efa-cuda-10.0/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n
100
```

3. Você pode confirmar se EFA está ativo como o provedor subjacente para NCCL quando o log NCCL\_DEBUG é impresso.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

As seguintes informações adicionais são exibidas ao usar uma instância p4d.24xlarge.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-ofi-
nccl/xml/p4d-24xl-topo.xml
```

## Etapa 4: Instalar as aplicações de machine learning

Instale as aplicações de machine learning na instância temporária. O procedimento de instalação varia dependendo da aplicação de machine learning específica. Para obter mais informações sobre como instalar software em sua instância do Linux, consulte [Gerenciamento de software em sua instância do Linux](#).

### Note

Pode ser necessário consultar a documentação da sua aplicação de machine learning para obter instruções de instalação.

## Etapa 5: Criar um EFA e uma AMI habilitada para NCCL

Depois de instalar os componentes de software necessários, crie uma AMI que possa ser reutilizada para executar suas instâncias habilitadas para o EFA.

Para criar uma AMI a partir de sua instância temporária

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), Image (Imagen), Create image (Criar imagem).
4. Em Create image (Criar imagem), faça o seguinte:
  - a. Em Image name (Nome da imagem), insira um nome descritivo para a AMI.
  - b. (Opcional) Em Image description (Descrição da imagem), informe a descrição do propósito da AMI.
  - c. Escolha Create Image (Criar imagem).
5. No painel de navegação, selecione AMIs.
6. Encontre a AMI que você criou na lista. Aguarde até que o status mude de pending para available antes de continuar para a próxima etapa.

## Etapa 6: Encerrar a instância temporária

Neste ponto, você não precisa mais da instância temporária que você executou. É possível encerrar a instância para não incorrer mais em cobranças desnecessárias.

Para encerrar a instância temporária

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 temporária, escolha Actions (Ações), selecione Instance state (Estado da instância), Terminate instance (Encerrar instance).
4. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

## Etapa 7: Iniciar instâncias habilitadas para o EFA e para a NCCL em um placement group de cluster

Execute as instâncias habilitadas para EFA em um grupo de posicionamento de cluster usando a AMI habilitada para EFA criada e o grupo de segurança habilitado para EFA criado anteriormente.

Para executar as instâncias habilitadas para EFA e NCCL em um grupo de posicionamento de cluster.

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 AMI (Escolher uma AMI), selecione My AMIs (Minhas AMIs), localize a AMI criada anteriormente e escolha Select (Selecionar).
4. Na página Choose an Instance Type (Escolher um tipo de instância), escolha p3dn.24xlarge e selecione Next: Configure Instance Details (Próximo: configurar detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), faça o seguinte:
  - a. Em Number of instances (Número de instâncias), insira o número de instâncias habilitadas para EFA e NCCL que você deseja executar.
  - b. Em Network (Rede) e Subnet (Sub-rede), selecione a VPC e a sub-rede na qual executar as instâncias.
  - c. Em Placement group, selecione Add instance to placement group (Adicionar instância ao placement group).
  - d. Em Placement group name (Nome do grupo de posicionamento), selecione Add to a new placement group (Adicionar a um novo grupo de posicionamento) e, em seguida, insira um nome descritivo para o grupo de posicionamento. Em seguida, em Placement group strategy (Estratégia do grupo de posicionamento), selecione cluster.
  - e. Para EFA, escolha Enable (Habilitar).
  - f. Na seção Network Interfaces (Interfaces de rede), para dispositivo eth0, escolha New network interface (Nova interface de rede). Como opção, você pode especificar um endereço IPv4 principal e um ou mais endereços IPv4 secundários. Se estiver executando a instância em uma sub-rede que tenha um bloco CIDR IPv6 associado, você poderá especificar opcionalmente um endereço IPv6 principal e um ou mais endereços IPv6 secundários.
  - g. Escolha Next: Add Storage.
6. Na página Add Storage (Adicionar armazenamento), especifique os volumes para anexar às instâncias, além dos volumes especificados pela AMI (como o volume raiz). Depois, selecione Next: Add Tags (Próximo: adicionar tags).
7. Na página Add Tags (Adicionar tags), especifique tags para as instâncias, como nome amigável, e selecione Next: Configure Security Group (Próximo: Configurar grupo de segurança).

8. Na página Configure Security Group (Configurar grupo de segurança), para Assign a security group (Atribuir um grupo de segurança), selecione Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança que você criou anteriormente.
9. Escolha Review and Launch.
10. Na página Review Instance Launch (Revisar execução da instância), reveja as configurações, e escolha Launch (Executar) para escolher um par de chaves e executar a instâncias.

## Etapa 8: Habilitar SSH sem senha

Para permitir que suas aplicações sejam executadas em todas as instâncias do cluster, você deve habilitar o acesso SSH sem senha do nó líder para os nós membros. O nó líder é a instância a partir da qual você executa suas aplicações. As instâncias restantes no cluster são os nós membros.

Para habilitar SSH sem senha entre as instâncias no cluster

1. Selecione uma instância no cluster como o nó líder e conecte-se a ela.
2. Desabilite strictHostKeyChecking e habilite ForwardAgent no nó líder. Abra o `~/.ssh/config` usando o editor de texto de sua preferência e adicione o seguinte.

```
Host *
  ForwardAgent yes
Host *
  StrictHostKeyChecking no
```

3. Gere um par de chaves RSA.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

O par de chaves é criado no diretório do `$HOME/.ssh/`.

4. Altere as permissões da chave privada no nó líder.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Abra `~/.ssh/id_rsa.pub` usando seu editor de texto preferido e copie a chave.
6. Para cada nó de membro no cluster, faça o seguinte:
  - a. Conecte-se à instância.
  - b. Abra `~/.ssh/authorized_keys` usando o editor de texto de sua preferência e adicione a chave pública que você copiou anteriormente.
7. Para testar se o SSH sem senha está funcionando como esperado, conecte-se ao seu nó líder e execute o comando a seguir.

```
$ ssh member_node_private_ip
```

Você deve se conectar ao nó membro sem receber uma solicitação para inserir uma chave ou senha.

## Trabalhar com EFA

Você pode criar, usar e gerenciar um EFA como qualquer outra interface de rede elástica no Amazon EC2. No entanto, ao contrário das interfaces de rede elástica, os EFAs não podem ser anexados ou desanexados de uma instância em um estado em execução.

## Requisitos do EFA

Para usar um EFA, você deve fazer o seguinte:

- Escolha um dos [tipos de instância compatíveis \(p. 1046\)](#).
- Use uma das [AMIs compatíveis \(p. 1046\)](#).
- Instale os componentes de software de EFA. Para obter mais informações, consulte [Etapa 3: Instalar o software EFA \(p. 1049\)](#) e [Etapa 5: \(Opcional\) Instalar o Intel MPI \(p. 1052\)](#).
- Use um grupo de segurança que permite todo o tráfego de entrada e saída de e para o próprio grupo de segurança. Para obter mais informações, consulte [Etapa 1: Preparar um grupo de segurança habilitado para EFA \(p. 1048\)](#).

### Tópicos

- [Criar um EFA. \(p. 1079\)](#)
- [Associar um EFA a uma instância interrompida \(p. 1080\)](#)
- [Associar um EFA ao executar uma instância \(p. 1080\)](#)
- [Adicionar um EFA a um modelo de execução \(p. 1080\)](#)
- [Gerenciar endereços IP para um EFA \(p. 1080\)](#)
- [Alterar o grupo de segurança para um EFA \(p. 1081\)](#)
- [Desanexar um EFA \(p. 1081\)](#)
- [Visualizar EFAs \(p. 1081\)](#)
- [Excluir um EFA \(p. 1081\)](#)

## Criar um EFA.

Você pode criar um EFA em uma sub-rede de uma VPC. Você não pode mover o EFA para outra sub-rede depois que ela é criada e só pode anexá-la a instâncias interrompidas na mesma zona de disponibilidade.

Para criar um novo EFA 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. Em Description (Descrição), insira um nome descritivo para o EFA.
5. Para Subnet (Sub-rede), selecione a sub-rede na qual criar o EFA.
6. Para Private IP (IP privado), insira o endereço IPv4 privado principal. Se você não especificar um endereço IPv4, selecionaremos um endereço IPv4 privado disponível 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 Security groups, selecione um ou mais security groups.
9. Para EFA, selecione Enabled (Habilitado).
10. Escolha Yes, Create.

Para criar um novo EFA usando a AWS CLI

Use o comando `create-network-interface` e, para `interface-type`, especifique `efa`, conforme mostrado no exemplo a seguir.

```
aws ec2 create-network-interface --subnet-id subnet-01234567890 --description example_efa  
--interface-type efa
```

## Associar um EFA a uma instância interrompida

Você pode anexar um EFA a qualquer instância compatível que esteja no estado `stopped`. Você pode anexar um EFA a uma instância que esteja no estado `running`. Para obter mais informações sobre os tipos de instâncias compatíveis, consulte [Tipos de instâncias compatíveis \(p. 1046\)](#).

Anexe um EFA a uma instância da mesma forma como você anexa uma interface de rede a uma instância. Para obter mais informações, consulte [Anexar uma interface de rede a uma instância \(p. 1003\)](#).

## Associar um EFA ao executar uma instância

Para anexar um EFA existente ao executar uma instância (AWS CLI)

Use o comando `run-instances` e, para `NetworkInterfaceId`, especifique o ID do EFA, conforme mostrado no exemplo a seguir.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-  
type c5n.18xlarge --key-name my_key_pair --network-interfaces  
DeviceIndex=0,NetworkInterfaceId=efa_id,Groups=sg_id,SubnetId=subnet_id
```

Para anexar um novo EFA ao executar uma instância (AWS CLI)

Use o comando `run-instances` e, para `InterfaceType`, especifique o ID do `efa`, conforme mostrado no exemplo a seguir.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-  
type c5n.18xlarge --key-name my_key_pair --network-interfaces  
DeviceIndex=0,InterfaceType=efa,Groups=sg_id,SubnetId=subnet_id
```

## Adicionar um EFA a um modelo de execução

Você pode criar um modelo de execução que contenha informações de configuração necessárias para executar instâncias habilitadas para EFA. Para criar um modelo de execução habilitado para EFA, crie um novo modelo de execução e especifique um tipo de instância compatível, sua AMI habilitada para EFA e um grupo de segurança habilitado para EFA. Para obter mais informações, consulte [Conceitos básicos do EFA e MPI \(p. 1047\)](#).

Você pode aproveitar modelos de execução para executar instâncias habilitadas para EFA com outros produtos da AWS, como AWS Batch.

Para obter mais informações sobre como criar modelos de execução, consulte [Criar um modelo de execução \(p. 519\)](#).

## Gerenciar endereços IP para um EFA

É possível alterar os endereços IP associados a um EFA. Se tiver um endereço IP elástico, você poderá associá-lo a um EFA. Se seu EFA estiver provisionado em uma sub-rede que tenha um bloco CIDR IPv6 associado, você poderá atribuir um ou mais endereços IPv6 ao EFA.

Você atribui um endereço IP elástico (IPv4) e IPv6 a um EFA da mesma forma como atribui um endereço IP a uma interface de rede elástica. Para obter mais informações, consulte [Gerenciar endereços IP \(p. 1005\)](#).

## Alterar o grupo de segurança para um EFA

Você pode alterar o grupo de segurança associado a um EFA. Para habilitar a funcionalidade de desvio do sistema operacional, o EFA deve ser um membro de um grupo de segurança que permita todo o tráfego de entrada e saída de e para o próprio grupo de segurança.

Você pode alterar o grupo de segurança associado a um EFA da mesma forma como altera o grupo de segurança associado a uma interface de rede elástica. Para obter mais informações, consulte [Alterar o grupo de segurança \(p. 1006\)](#).

## Desanexar um EFA

Para desanexar um EFA de uma instância, primeiro você deve parar a instância. Você não pode desanexar um EFA de uma instância que está em estado de execução.

Você desanexa um EFA de uma instância da mesma maneira como desanexa uma interface de rede elástica de uma instância. Para obter mais informações, consulte [Desanexar uma interface de rede de uma instância \(p. 1004\)](#).

## Visualizar EFAs

Você pode ver todos os EFAs da sua conta.

Você visualiza EFAs da mesma maneira como visualiza interfaces de rede elástica. Para obter mais informações, consulte [Visualizar detalhes sobre uma interface de rede \(p. 1002\)](#).

## Excluir um EFA

Para excluir um EFA, você deve primeiro separá-lo da instância. Você não pode excluir um EFA enquanto está anexado a uma instância.

Você exclui EFAs da mesma maneira como visualiza interfaces de rede elástica. Para obter mais informações, consulte [Excluir uma interface de rede \(p. 1008\)](#).

## Monitorar um EFA

Você pode usar os seguintes recursos para monitorar a performance dos seus Elastic Fabric Adapters.

### Logs de fluxo do Amazon VPC

Você pode criar um log de fluxo da Amazon VPC para capturar informações sobre o tráfego de entrada e saída de um EFA. Os dados de log de fluxo podem ser publicados no Amazon CloudWatch Logs e no Amazon S3. Após criar um log de fluxo, você poderá recuperar e visualizar seus dados no destino selecionado. Para obter mais informações, consulte [Logs de fluxo da VPC](#) no Guia do usuário da Amazon VPC.

Você cria um log de fluxo para um EFA da mesma forma como cria um log de fluxo para uma interface de rede elástica. Para mais informações, consulte [Criação de um log de fluxo](#) no Guia do usuário da Amazon VPC.

Nas entradas do log de fluxo, o tráfego do EFA é identificado por `srcAddress` e `destAddress`, ambos formatados como endereços MAC, conforme mostrado no exemplo a seguir.

```
version accountId eniId      srcAddress          destAddress        sourcePort destPort
protocol packets bytes start      end            action log-status
2           3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -       -
9           5689   1521232534 1524512343 ACCEPT OK
```

## Amazon CloudWatch

O Amazon CloudWatch fornece métricas que permitem monitorar os EFAs em tempo real. Você pode coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Para obter mais informações, consulte [Monitorar instâncias usando o CloudWatch \(p. 872\)](#).

## Verificar o instalador EFA usando uma soma de verificação

Como opção, você pode verificar o tarball EFA (arquivo .tar.gz) usando uma soma de verificação MD5 ou SHA256. Recomendamos que você faça isso para verificar a identidade do fornecedor do software e para verificar se a aplicação não foi alterada ou corrompida desde que foi publicada.

Como verificar o tarball

Use o utilitário md5sum para a soma de verificação MD5 ou o utilitário sha256sum para a soma de verificação SHA256 e especifique o nome do arquivo tarball. Você deve executar o comando a partir do diretório no qual salvou o arquivo tarball.

- MD5

```
$ md5sum tarball_filename.tar.gz
```

- SHA256

```
$ sha256sum tarball_filename.tar.gz
```

Os comandos devem retornar um valor de soma de verificação no formato a seguir.

```
checksum_value tarball_filename.tar.gz
```

Compare o valor de soma de verificação retornado pelo comando com o valor de soma de verificação fornecido na tabela abaixo. Se as somas de verificação corresponderem, então é seguro executar o script de instalação. Se as somas de verificação não corresponderem, não execute o script de instalação e entre em contato com o AWS Support.

Por exemplo, o comando a seguir verifica o tarball EFA 1.9.4 usando a soma de verificação SHA256.

```
$ sha256sum aws-efa-installer-1.9.4.tar.gz
```

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

A tabela a seguir lista as somas de verificação para versões recentes do EFA.

Versão	Faça download do URL	Somas de verificação
EFA 1.13.0	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.13.0.tar.gz">https://efa-installer.amazonaws.com/ aws-efa-installer-1.13.0.tar.gz</a>	MD5: c91d16556f4fd53becadbb345828221e  SHA256: ad6705eb23a3fce44af3afc0f7643091595653a72

**Amazon Elastic Compute Cloud Manual**  
 do usuário para instâncias do Linux  
 Verificar o instalador EFA usando uma soma de verificação

Versão	Faça download do URL	Somas de verificação
EFA 1.12.3	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.12.3.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.12.3.tar.gz</a>	MD5: 818aee81f097918cfaebd724eddea678  SHA256: 2c225321824788b8ca3fbc118207b944cdb096b84
EFA 1.12.2	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.12.2.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.12.2.tar.gz</a>	MD5: 956bb1fc5ae0d6f0f87d2e481d49fccf  SHA256: 083a868a2c212a5a4fcf3e4d732b685ce39cccb3c
EFA 1.12.1	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.12.1.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.12.1.tar.gz</a>	MD5: f5bfe52779df435188b0a2874d0633ea  SHA256: 5665795c2b4f09d5f3f767506d4d4c429695b36d4
EFA 1.12.0	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.12.0.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.12.0.tar.gz</a>	MD5: d6c6b49fafb39b770297e1cc44fe68a6  SHA256: 28256c57e9ecc0b0778b41c1f777a9982b4e8ae7
EFA 1.11.2	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.11.2.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.11.2.tar.gz</a>	MD5: 2376cf18d1353a4551e35c33d269c404  SHA256: a25786f98a3628f7f54f7f74ee2b39bc6734ea937
EFA 1.11.1	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.11.1.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.11.1.tar.gz</a>	MD5: 026b0d9a0a48780cc7406bd51997b1c0  SHA256: 6cb04baf5ffc58ddf319e956b5461289199c8dd80
EFA 1.11.0	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.11.0.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.11.0.tar.gz</a>	MD5: 7d9058e010ad65bf2e14259214a36949  SHA256: 7891f6d45ae33e822189511c4ea1d14c9d54d000f
EFA 1.10.1	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.10.1.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.10.1.tar.gz</a>	MD5: 78521d3d668be22976f46c6fecc7b730  SHA256: 61564582de7320b21de319f532c3a677d26cc4678
EFA 1.10.0	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.10.0.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.10.0.tar.gz</a>	MD5: 46f73f5a7afe41b4bb918c81888fefef9  SHA256: 136612f96f2a085a7d98296da0afb6fa807b38142

Versão	Faça download do URL	Somas de verificação
EFA 1.9.5	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.9.5.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.9.5.tar.gz</a>	MD5: 95edb8a209c18ba8d250409846eb6ef4  SHA256: a4343308d7ea4dc943ccc21bcebed913e8868e59b
EFA 1.9.4	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.9.4.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.9.4.tar.gz</a>	MD5: f26dd5c350422c1a985e35947fa5aa28  SHA256: 1009b5182693490d908ef0ed2c1dd4f813cc310a5
EFA 1.9.3	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.9.3.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.9.3.tar.gz</a>	MD5: 95755765a097802d3e6d5018d1a5d3d6  SHA256: 46ce732d6f3fcc9edf6a6e9f9df0ad136054328e2
EFA 1.8.4	<a href="https://efa-installer.amazonaws.com/aws-efa-installer-1.8.4.tar.gz">https://efa-installer.amazonaws.com/aws-efa-installer-1.8.4.tar.gz</a>	MD5: 85d594c41e831afc6c9305263140457e  SHA256: 0d974655a09b213d7859e658965e56dc4f23a0eee

## 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

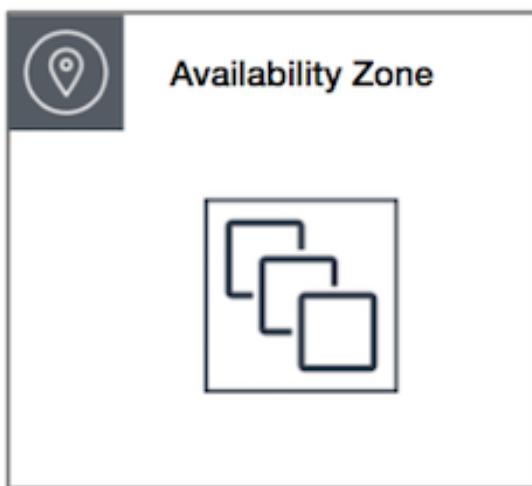
- [Placement groups de cluster \(p. 1085\)](#)
- [Placement groups de partição \(p. 1086\)](#)
- [Placement groups de distribuição \(p. 1086\)](#)
- [Regras e limitações do placement group \(p. 1087\)](#)
- [Criar um placement group. \(p. 1088\)](#)
- [Marcar um placement group \(p. 1089\)](#)
- [Executar instâncias em um placement group \(p. 1092\)](#)

- Descrever instâncias em um placement group (p. 1093)
- Alterar o placement group de uma instância (p. 1094)
- Excluir um placement group. (p. 1095)

## 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 \(p. 1015\)](#).

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.

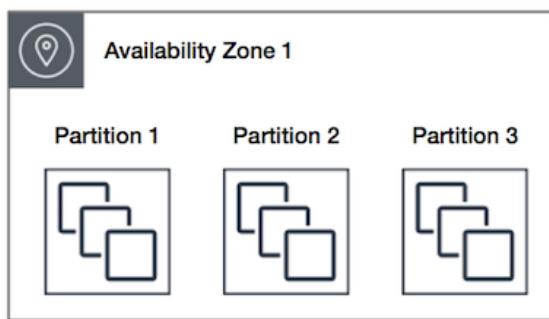
Se você interrompe uma instância em um placement group e depois a inicia novamente, ela ainda é executada no placement group. Contudo, ocorrerá uma falha na inicialização se não houver capacidade suficiente para a instância.

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 separadas umas 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 \(p. 484\)](#) e as [Instâncias reservadas de zona \(p. 347\)](#) 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 \(p. 204\)](#), exceto as instâncias [expansíveis \(p. 228\)](#) (por exemplo, T2) e [instâncias Mac1 \(p. 264\)](#).
  - As seguintes instâncias da [geração anterior \(p. 208\)](#): 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 \(p. 1552\)](#).

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 \(p. 1560\)](#).

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 \(p. 1556\)](#).
  - 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 \(p. 1087\)](#) 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 \(p. 589\)](#) todas as instâncias executadas no placement group, [movê-las \(p. 1095\)](#) para outro placement group ou [removê-las \(p. 1095\)](#) 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 permitido 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 do Windows, alterne para esta página no guia Guia do usuário do Amazon EC2 para instâncias do Windows: [Unidade de transmissão máxima de rede \(MTU\) para sua instância do EC2](#).

#### Tópicos

- [Frames jumbo \(9.001 MTU\) \(p. 1097\)](#)
- [Path MTU Discovery \(p. 1098\)](#)
- [Verificar o MTU do caminho entre dois hosts \(p. 1098\)](#)
- [Verificar e definir o MTU na instância do Linux \(p. 1099\)](#)
- [Troubleshoot \(p. 1100\)](#)

## 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 \(p. 1084\)](#).

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. 211) 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. A MTU do caminho é o tamanho de pacote máximo suportado no caminho entre o host de origem e o host de receção.

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 `tracepath`, que é parte do pacote `iutils` disponível por padrão em várias distribuições Linux, inclusive Amazon Linux.

Para verificar o MTU do caminho usando o `tracepath`

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 `amazon.com`.

```
[ec2-user ~]$ tracepath amazon.com
1?: [LOCALHOST]          pmtu 9001
1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)    0.187ms pmtu 1500
1:  no reply
2:  no reply
3:  no reply
4:  100.64.16.241 (100.64.16.241)                                0.574ms
5:  72.21.222.221 (72.21.222.221)                                84.447ms asymm 21
6:  205.251.229.97 (205.251.229.97)                                79.970ms asymm 19
```

```
7: 72.21.222.194 (72.21.222.194)          96.546ms asymm 16
8: 72.21.222.239 (72.21.222.239)          79.244ms asymm 15
9: 205.251.225.73 (205.251.225.73)         91.867ms asymm 16
...
31: no reply
    Too many hops: pmtu 1500
    Resume: pmtu 1500
```

Neste exemplo, o MTU do caminho é 1500.

## Verificar e definir o MTU na instância do Linux

Algumas instâncias são configuradas para usar frames jumbo, e outras são configuradas 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 seu caso de uso, recomendamos verificar se sua instância se comportará da maneira como você espera. Você pode usar os procedimentos desta seção para verificar a configuração de MTU da interface de rede e modificá-la, se necessário.

Para verificar a configuração de MTU em uma instância do Linux

Você pode verificar o valor atual de MTU usando o comando ip a seguir. Observe que, na saída de exemplo, **mtu 9001** indica que essa instância usa frames jumbo.

```
[ec2-user ~]$ ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode DEFAULT
    group default qlen 1000
        link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

Para definir o valor de MTU em uma instância do Linux

1. Você pode definir o valor de MTU usando o comando ip. Os comandos a seguir definem o valor de MTU desejado para 1500, mas você poderia usar 9001.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
```

2. (Opcional) Para persistir a configuração de MTU de rede após a reinicialização, modifique os arquivos de configuração a seguir com base no tipo de sistema operacional.

- No Amazon Linux 2, adicione a linha a seguir ao arquivo /etc/sysconfig/network-scripts/ifcfg-eth0:

```
MTU=1500
```

Adicione a linha a seguir ao arquivo /etc/dhcp/dhclient.conf:

```
request subnet-mask, broadcast-address, time-offset, routers, domain-name, domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-servers;
```

- Para Amazon Linux, adicione as linhas a seguir ao seu arquivo /etc/dhcp/dhclient-eth0.conf.

```
interface "eth0" {
    supersede interface-mtu 1500;
}
```

- Para outras distribuições de Linux, consulte a documentação específica.

3. (Opcional) Reinicie sua instância e verifique se a configuração de MTU está correta.

## 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 \(p. 1100\)](#).

## Documentação da Amazon VPC

Para obter mais informações sobre uma Amazon VPC, consulte a seguinte documentação.

Guia	Descrição
<a href="#">Manual do usuário da Amazon VPC</a>	Descreve os principais conceitos e disponibiliza instruções para uso dos recursos do Amazon VPC.
<a href="#">Amazon VPC Peering Guide</a>	Descreve as conexões pares da VPC e disponibiliza instruções para usá-las.
<a href="#">Gateways de trânsito da Amazon VPC</a>	Descreve gateways de trânsito e fornece instruções para configurá-los e usá-los.
<a href="#">AWS Site-to-Site VPN Guia do usuário</a>	Descreve conexões do Site-to-Site VPN e fornece instruções para configurá-las e usá-las.

## 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"
                }
            ],
            "AttributeName": "supported-platforms",
        }
    ]
}
```

## 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 \(p. 1120\)](#).

## 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.
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.

**Amazon Elastic Compute Cloud Manual**  
 do usuário para instâncias do Linux  
 Diferenças entre instâncias no EC2-Classic e em uma VPC

Característica	EC2-Classic	VPC padrão	VPC não padrão
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.
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:

```
grep nameserver /etc/resolv.conf
```

## 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 [Desassociar um endereço IP elástico \(p. 980\)](#).

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 \(p. 983\)](#).

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 \(p. 1109\)](#).

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 recriar 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 \(p. 1120\)](#).

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 <a href="#">Migrar um endereço IP elástico do EC2-Classic (p. 1106)</a> .

Recurso	Observações
Instância	<p>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.</p> <p>Não é possível migrar uma instância do EC2-Classic para uma VPC. Contudo, é possível migrar sua aplicação de uma instância na EC2-Classic para uma instância em uma VPC. Para obter mais informações, consulte <a href="#">Migre do EC2-Classic para uma VPC (p. 1120)</a>.</p>
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	<p>Você pode alterar a plataforma de rede para Instâncias reservadas do EC2-Classic para uma VPC. Para obter mais informações, consulte <a href="#">Modificar a Instâncias reservadas (p. 375)</a>.</p>
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 <a href="#">Crie um grupo de segurança (p. 1231)</a>.</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 \(p. 1120\)](#).

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 \(p. 1109\)](#)
- [Limitações do ClassicLink \(p. 1112\)](#)
- [Trabalhar com ClassicLink \(p. 1112\)](#)
- [Exemplos de políticas do IAM para ClassicLink \(p. 1116\)](#)
- [Exemplo: configuração do grupo de segurança do ClassicLink para uma aplicação Web de três níveis \(p. 1118\)](#)

## 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 \(p. 1114\)](#).

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 \(p. 1115\)](#).

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 \(p. 1116\)](#).

## 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 \(p. 1118\)](#).

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 de 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 \(p. 1111\)](#).
- 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 \(p. 1113\)](#)
- [Criar uma VPC com ClassicLink habilitado \(p. 1113\)](#)
- [Vincular a uma instância a uma VPC \(p. 1114\)](#)
- [Vincular uma instância a uma VPC na execução \(p. 1114\)](#)
- [Visualizar suas VPCs habilitadas para ClassicLink e as instâncias vinculadas \(p. 1114\)](#)
- [Habilitar o suporte a DNS do ClassicLink \(p. 1115\)](#)
- [Desabilitar o suporte a DNS do ClassicLink \(p. 1115\)](#)
- [Desvincular uma instância de uma VPC \(p. 1115\)](#)
- [Desabilitar ClassicLink para uma VPC \(p. 1116\)](#)

## 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 \(p. 1111\)](#).

### 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 \(p. 1115\)](#).

## 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 \(p. 1115\)](#).

## 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 \(p. 1115\)](#).

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 \(p. 1102\)](#).
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. \(p. 510\)](#).

## 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 \(p. 1116\)](#)
- [Habilitar e desabilitar uma VPC para o ClassicLink \(p. 1117\)](#)
- [Vincular instâncias \(p. 1117\)](#)
- [Desvincular instâncias \(p. 1118\)](#)

### 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:AssociateClassicLinkVpc",  
            "Resource": "arn:aws:ec2:region:account:vpc/vpc-1a2b3c4d",  
            "Condition": {  
                "StringEquals": {  
                    "ec2:ResourceTag/group": "sg-1122aabb,sg-aabb2233"  
                }  
            }  
        }  
    ]  
}
```

```
    "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.

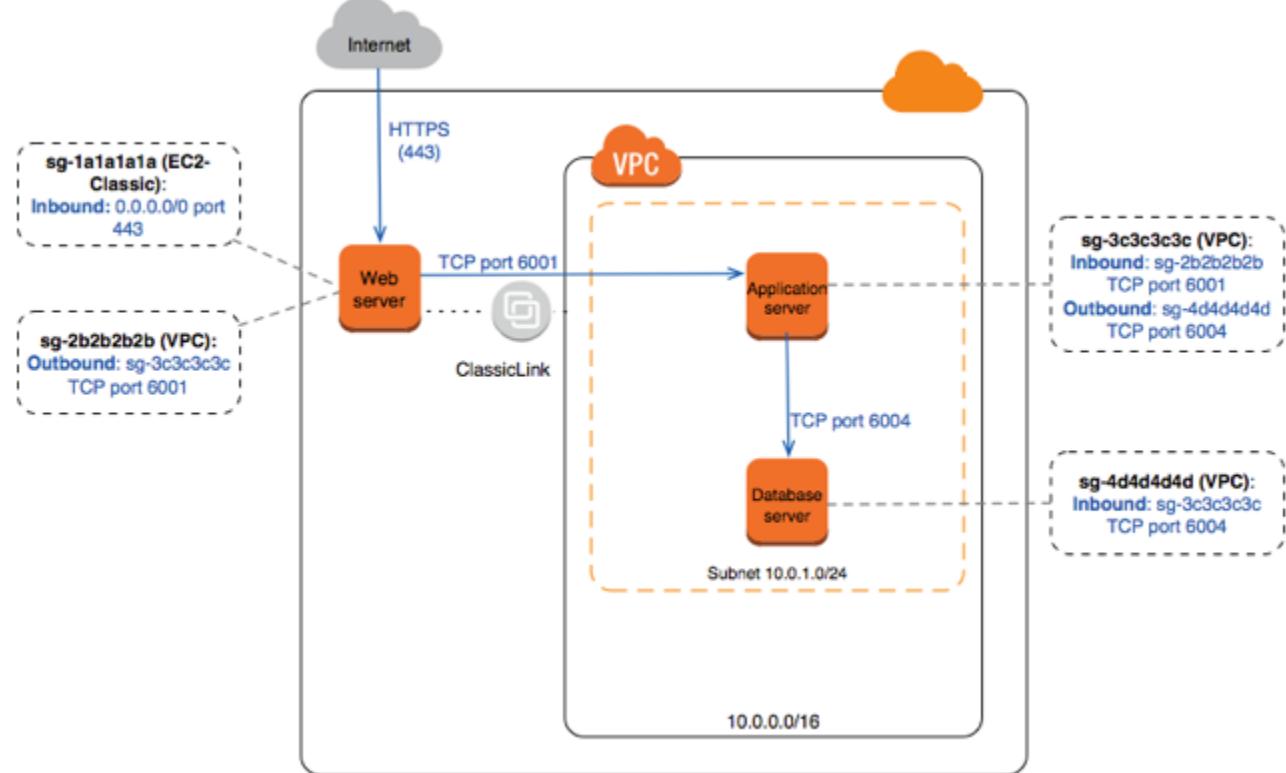
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DetachClassicLinkVpc",
            "Resource": [
                "arn:aws:ec2:region:account:instance/*"
            ],
            "Condition": {
                "StringEquals": {
                    "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 \(p. 1107\)](#). 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 \(p. 1121\)](#)
- [Migrar seus recursos para uma VPC \(p. 1122\)](#)
- [Usar ClassicLink para uma migração incremental \(p. 1126\)](#)
- [Exemplo: Migrar uma aplicação Web simples \(p. 1127\)](#)

## 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 \(p. 1121\)](#)
- [Criar uma nova conta da AWS \(p. 1121\)](#)
- [Converter a conta da AWS existente em somente VPC \(p. 1121\)](#)

## 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 \(p. 1101\)](#).

## 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 \(p. 1122\)](#).

#### 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](http://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 \(p. 1122\)](#)
- [Endereços IP elásticos \(p. 1123\)](#)
- [AMIs e instâncias \(p. 1123\)](#)
- [Instâncias de banco de dados do Amazon RDS \(p. 1126\)](#)

## 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 Linux \(p. 1225\)](#).

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 Linux \(p. 1225\)](#).

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 \(p. 1106\)](#).

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 \(p. 1124\)](#)
- [Criar uma AMI \(p. 1124\)](#)
- [\(Opcional\) Compartilhar ou copiar a AMI \(p. 1125\)](#)

- [\(Opcional\) Armazenar os dados em volumes do Amazon EBS \(p. 1125\)](#)
- [Executar uma instância na VPC \(p. 1125\)](#)

## 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 <a href="#">Criar uma AMI do Linux baseada no Amazon EBS</a> .

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 <a href="#">Criar uma AMI do Linux com armazenamento de instâncias</a> .
Armazenamento de instâncias	Converta sua instância com armazenamento de instâncias em uma instância baseada em EBS. Para obter mais informações, consulte <a href="#">Converter a AMI com armazenamento de instâncias em uma AMI baseada no Amazon EBS</a> .

#### (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 \(p. 96\)](#).

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 \(p. 144\)](#).

#### (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 \(p. 1250\)](#)
- [Crie um volume do Amazon EBS. \(p. 1274\)](#)
- [Vincular um volume de Amazon EBS a uma instância \(p. 1277\)](#)

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 \(p. 1307\)](#). 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 \(p. 1275\)](#).

#### 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](#). No entanto, verifique se o tipo de instância é compatível com o tipo de virtualização que sua AMI oferece (PV ou HVM). Para obter mais informações sobre virtualização de HVM e PV, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#).

#### 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. \(p. 510\)](#).

## 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 \(p. 1109\)](#).

### Tarefas

- [Etapa 1: Preparar a sequência de migração \(p. 1126\)](#)
- [Etapa 2: Habilitar a VPC para o ClassicLink \(p. 1127\)](#)
- [Etapa 3: Vincular as instâncias do EC2-Classic à VPC \(p. 1127\)](#)
- [Etapa 4: Concluir a migração da VPC \(p. 1127\)](#)

### 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 \(p. 1122\)](#).

## 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.

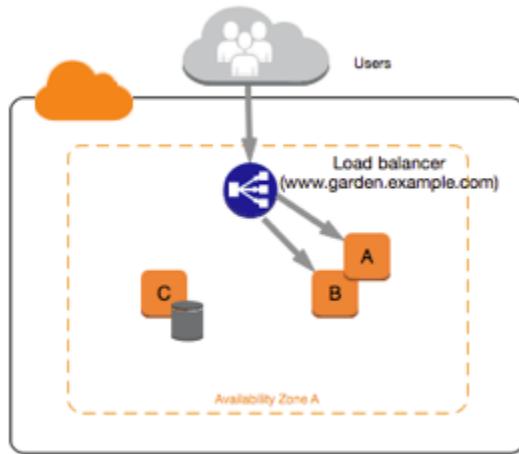
Após habilitar a comunicação interna entre o EC2-Classic e as instâncias de VPC, você deverá atualizar sua aplicação para apontar para o serviço migrado em sua VPC, em vez do serviço na plataforma do EC2-Classic. As etapas exatas dependem do design de sua aplicação. Geralmente, isso inclui a atualização 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.

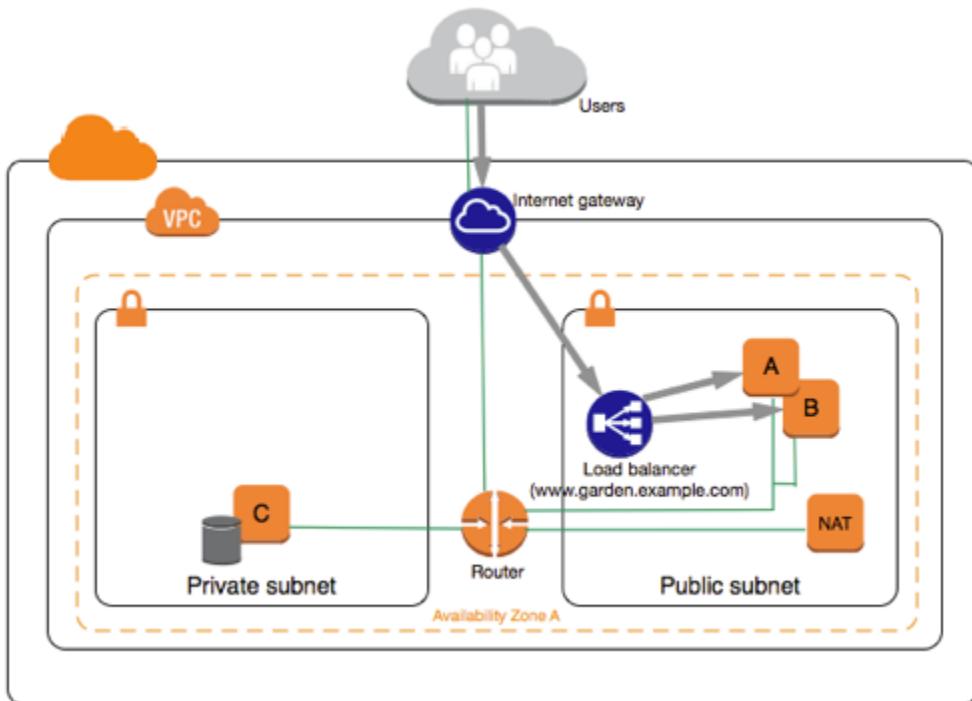
## Exemplo: Migrar uma aplicação Web simples

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 \(p. 1122\)](#).

**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 \(p. 1124\)](#).
- 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 \(p. 1106\)](#).
- 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 \(p. 1131\)](#).
  - 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 \(p. 1246\)](#).
  - 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.

## 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 \(p. 1136\)](#)
- [Pares de chaves do Amazon EC2 e instâncias do Linux \(p. 1209\)](#)
- [Grupos de segurança do Amazon EC2 para instâncias do Linux \(p. 1225\)](#)
- [Gerenciamento de atualizações no Amazon EC2 \(p. 1246\)](#)
- [Validação de conformidade do Amazon EC2 \(p. 1246\)](#)

## 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 \(p. 1225\)](#). Por exemplo, você pode permitir tráfego apenas de intervalos de endereços de sua rede corporativa.
- Use sub-redes privadas para as instâncias que não devem ser acessadas diretamente pela Internet. Use um bastion host ou gateway NAT para acesso à Internet em uma instância em uma sub-rede privada.
- 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 [EC2 Instance Connect \(p. 541\)](#) para conectar-se a suas instâncias usando Secure Shell (SSH) sem a necessidade de compartilhar e gerenciar chaves SSH.
- Use o [Gerenciador de sessões do AWS Systems Manager](#) para acessar suas instâncias remotamente em vez de abrir portas SSH de entrada e chaves SSH de gerenciamento.
- Use o [Run Command do AWS Systems Manager](#) para automatizar tarefas administrativas em vez de abrir portas SSH de entrada e chaves SSH de gerenciamento.

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 \(p. 1418\)](#).

### 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 | C6gn
  - Memória otimizada: R5dn | R5n | alta memória (u-\*), apenas virtualizada
  - Otimizada para armazenamento: D3 | D3en | I3en
  - Computação acelerada: G4ad | G4dn | Inf1 | P3dn | P4d
- 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 SSH fornece um canal de comunicação seguro para o acesso remoto às instâncias do Linux, 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.

## 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 \(p. 1137\)](#)
- [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 Linux \(p. 1205\)](#)

## 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 Linux \(p. 1205\)](#).

## 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 \(p. 95\)](#).

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 \(p. 1319\)](#).

## 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	<a href="#">Sintaxe da política (p. 1140)</a>
Definir ações em sua política	<a href="#">Ações do Amazon EC2 (p. 1141)</a>
Definir recursos específicos em sua política	<a href="#">Nomes de recurso da Amazon (ARNs) para o Amazon EC2 (p. 1142)</a>
Aplicar condições ao uso dos recursos	<a href="#">Chaves de condição do Amazon EC2 (p. 1143)</a>
Trabalhar com permissões disponíveis em nível de recurso para o Amazon EC2	<a href="#">Ações, recursos e chaves de condição para o Amazon EC2</a>

Tarefa	Tópico
Testar a política	<a href="#">Verificar se os usuários têm as permissões necessárias (p. 1144)</a>
Gerar uma política do IAM	<a href="#">Gerar políticas com base na atividade de acesso</a>
Políticas de exemplo para uma CLI ou SDK	<a href="#">Políticas de exemplo para trabalhar com a AWS CLI ou um AWS SDK (p. 1147)</a>
Políticas de exemplo para o console do Amazon EC2	<a href="#">Políticas de exemplo para trabalhar no console do Amazon EC2 (p. 1185)</a>

## 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 \(p. 1144\)](#).

## 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 \(p. 1553\)](#) 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 \(p. 1150\)](#)
- [Trabalhar com snapshots \(p. 1153\)](#)

- Executar instâncias (RunInstances) (p. 1160)
- 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](#).

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": {  
                "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.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Allow",  
            "Action": [  
                "ec2:DescribeInstances",  
                "ec2:DescribeImages",  
                "ec2:DescribeKeyPairs",  
                "ec2:DescribeSecurityGroups",  
                "ec2:DescribeAvailabilityZones",  
                "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](#).

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": {  
                "StringEquals": {  
                    "ec2:ResourceTag/encrypted": "true"  
                }  
            }  
        }  
    ]  
}
```

```
        "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 \(p. 1144\)](#).

```
{
    "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 \(p. 1144\)](#).

```
{  
    "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/*"
            ]
        },
        {
            "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 `CreateS snapshots` 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:CreateS snapshots",
            "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:*:instance/*",  
                "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: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:***:volume/*"  
            ],  
            "Condition": {  
                "Bool": {  
                    "ec2:Encrypted": "true"  
                }  
            }  
        },  
        {  
            "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 \(p. 1144\)](#).

```
{
    "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"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment" : "production"
                }
            }
        }
    ]
}
```

```
[  
  "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/*"  
            ]  
        }  
    ]  
}
```

```
        "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::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": "*"  
        }  
    ]  
}
```

```
    "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",
        "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 excluam tags específicas de um recurso. Por exemplo, a política a seguir permite que os usuários excluam 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 excluam 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 \(p. 649\)](#) 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 \(RunInstances\) \(p. 1160\)](#).

**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 \(p. 1144\)](#). 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 \(RunInstances\) \(p. 1160\)](#). 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": {  
                "aws:RequesterId": "  
                "aws:SourceIdentity": "  
            }  
        }  
    }  
}
```

```
        "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 etiquete instâncias para você. Para obter mais informações, consulte [Função vinculada ao serviço para Frota do EC2](#) (p. 731).

## 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. 762).

## 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. 401).

## 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.

Ao criar funções do IAM, associe políticas do IAM de privilégio mínimo que restringem o acesso às chamadas de API específicas exigidas pela aplicação.

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 \(p. 1197\)](#)
- [Conceder uma permissão de usuário do IAM para transmitir uma função do IAM para uma instância \(p. 1198\)](#)
- [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

```
[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/iam/security-credentials/s3access
```

### IMDSv1

```
[ec2-user ~]$ curl 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 \(p. 649\)](#). Para obter informações sobre o endereço IP dos metadados da instância, consulte [Recuperar metadados da instância \(p. 657\)](#).

## 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 \(p. 1199\)](#)
- [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"
    }
}
```

- 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": ["*"]
        }
    ]
}
```

- 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
```

- 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"
    }
}
```

- 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-IAIMInstanceProfile](#)

## 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

```
[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/iam/security-credentials/role_name
```

#### IMDSv1

```
[ec2-user ~]$ curl 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 o 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"  
        }  
    }  
}
```

```
        "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 Linux

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 SSH. 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 \(p. 1229\)](#) e [Os security groups personalizados \(p. 1230\)](#). 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 SSH no endereço IPv4 público de seu computador. Para permitir tráfego do SSH 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 Windows, consulte [Como autorizar tráfego de entrada para suas instâncias Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## 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 SSH. 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.

Decida se você oferecerá suporte ao acesso SSH às suas instâncias usando o EC2 Instance Connect. Se não usar o EC2 Instance Connect, considere desinstalá-lo ou negar a seguinte ação em suas políticas do IAM: `ec2-instance-connect:SendSSHPublicKey`. Para obter mais informações, consulte [Desinstalar o EC2 Instance Connect \(p. 551\)](#) e [Configurar permissões do IAM para o EC2 Instance Connect \(p. 546\)](#).

## Adicionar uma regra para o tráfego de entrada do SSH a uma instância do Linux

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 Linux no seu endereço IP usando o SSH.

### New console

Para adicionar uma regra a um grupo de segurança para tráfego de entrada do SSH 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 SSH.
  - 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. Seleccione Save rules (Salvar regras).

#### Old console

Para adicionar uma regra a um grupo de segurança para tráfego de entrada do SSH 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 SSH 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 SSH.

#### New console

Para adicionar uma regra a um grupo de segurança para tráfego de entrada do SSH 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 SSH.
  - 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 SSH 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 SSH.
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 22 --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="22"; ToPort="22";  
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 Linux

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 Linux, a chave privada permite usar o SSH com segurança na 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 \(p. 517\)](#). Se você planeja se conectar à instância usando SSH, deverá especificar um par de chaves. É possível escolher um par de chaves existente ou criar um novo. Quando a instância é inicializada pela primeira vez, a chave pública especificada na inicialização é colocada na instância do Linux em uma entrada dentro de `~/.ssh/authorized_keys`. Ao conectar-se à instância do Linux usando SSH, você deve especificar a chave privada que corresponde à chave pública para fazer login. Para obter mais informações sobre como se conectar à sua instância, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#). Para obter mais informações sobre pares de chaves e instâncias do Windows, consulte [Pares de chaves do Amazon EC2 e instâncias do Windows](#) no Manual do usuário do Amazon EC2 para instâncias do Windows.

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 Linux em caso de perda da chave privada \(p. 1220\)](#).

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 \(p. 1212\)](#)
- [Etiquetar uma chave pública \(p. 1213\)](#)
- [Recuperar a chave pública da chave privada \(p. 1215\)](#)
- [Recuperar a chave pública por meio de metadados de instância \(p. 1216\)](#)
- [Localizar a chave pública em uma instância \(p. 1216\)](#)
- [Identificar o par de chaves que foi especificado na execução \(p. 1217\)](#)
- [Verificar a impressão digital do par de chaves \(p. 1217\)](#)
- [Adicionar ou substituir um par de chaves na sua instância \(p. 1218\)](#)
- [Excluir o par de chaves \(p. 1219\)](#)
- [Excluir uma chave pública de uma instância \(p. 1220\)](#)
- [Conectar-se à instância do Linux em caso de perda da chave privada \(p. 1220\)](#)

## 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 marcação à chave pública, escolha Adicionar marcação, e insira a chave e o valor da marcação. 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.

10. Se você usar um cliente SSH em um computador macOS ou Linux para conectar-se à instância do Linux, use o seguinte comando para definir as permissões do arquivo de chave privada de maneira que apenas você possa lê-lo.

```
chmod 400 my-key-pair.pem
```

Se você não definir essas permissões, não poderá conectar-se à instância usando esse par de chaves. Para obter mais informações, consulte [Erro: arquivo de chave privada desprotegido \(p. 1579\)](#).

## AWS CLI

### Como criar o par de chaves

1. 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.

--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
```

2. Se você usar um cliente SSH em um computador macOS ou Linux para conectar-se à instância do Linux, use o seguinte comando para definir as permissões do arquivo de chave privada de maneira que apenas você possa lê-lo.

```
chmod 400 my-key-pair.pem
```

Se você não definir essas permissões, não poderá conectar-se à instância usando esse par de chaves. Para obter mais informações, consulte [Erro: arquivo de chave privada desprotegido \(p. 1579\)](#).

## PowerShell

### Como criar o par de chaves

## Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2

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 em `~/.ssh/authorized_keys`). Se você se conectar usando SSH enquanto usa a API EC2 Instance Connect, o formato do SSH2 também será compatível.
  - 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. Se você se conectar usando SSH enquanto usa a API EC2 Instance Connect, os tamanhos compatíveis serão 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, `~/.ssh/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, `~/.ssh/my-key-pair.pem`.

**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.

## Etiqetar 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 \(p. 1552\)](#).

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 \(p. 1556\)](#).
  - 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.

```
$ 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.

```
$ 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.

```
$ 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

No computador Linux ou macOS local, você pode usar o comando ssh-keygen para recuperar a chave pública de seu par de chaves. Especifique o caminho onde você fez download de sua chave privada (o arquivo .pem).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

O comando retorna a chave pública, como mostrado no exemplo a seguir.

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxzb/wB96xb1FveSFJuOp/d6RJhJOI0iBXr
lsLnBITntckij7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
gaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUzofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Se o comando falhar, execute o comando a seguir para verificar se você alterou as permissões no arquivo de par de chaves privadas de forma que somente você possa visualizá-lo.

```
chmod 400 my-key-pair.pem
```

## 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.

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/public-keys/0/openssh-key
```

Veja a seguir um exemplo de saída.

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBITntckiJ7FbtJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221Cb5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb70z1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE my-key-pair
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Veja a seguir um exemplo de saída.

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBITntckiJ7FbtJMxLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0Fzz
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221Cb5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb70z1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE 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 \(p. 657\)](#).

## Localizar a chave pública em uma instância

Ao executar uma instância, um [par de chaves será solicitado \(p. 517\)](#). Se você planeja se conectar à instância usando SSH, deverá especificar um par de chaves. Quando a instância é inicializada pela primeira vez, o conteúdo da chave pública especificada na inicialização é colocado na instância do Linux em uma entrada dentro de `~/.ssh/authorized_keys`.

Como localizar a chave pública em uma instância

1. [Conecte-se à sua instância. \(p. 535\)](#)
2. Na janela do terminal, abra o arquivo `authorized_keys` usando seu editor de texto favorito (como vim ou nano).

```
[ec2-user ~]$ nano ~/.ssh/authorized_keys
```

O arquivo `authorized_keys` é aberto, exibindo a chave pública seguida pelo nome do par de chaves. A seguir está uma entrada de exemplo do par de chaves chamado de `my-key-pair`.

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQClksfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS706V  
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gu8jEzoOWbkm4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr  
lsLnBITntckij7fbtxJMXLvvwJryDU1lBMTjYtwB+QhYXUMOzce5pjz5/i8SeJtjnV3iAoG/cQk+0Fzz  
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb  
BQoQzd8v7yeb7Oz1PnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE my-key-pair
```

## Identificar o par de chaves que foi especificado na execução

Ao executar uma instância, um [par de chaves será solicitado \(p. 517\)](#). Se você planeja se conectar à instância usando SSH, 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
```

## Adicionar ou substituir um par de chaves na sua instância

Você pode alterar o par de chaves usado para acessar a conta de sistema padrão de sua instância adicionando uma nova chave pública na instância ou substituindo a chave pública (excluindo a chave pública existente e adicionando uma nova) na instância. Você pode fazer isso pelas seguintes razões:

- Se um usuário da sua organização requisitar acesso à conta do usuário no sistema usando um par de chaves separado, você poderá adicionar a chave pública à sua instância.
- Se alguém tiver uma cópia da chave privada (arquivo .pem) e você quiser impedir que essa pessoa se conecte à sua instância (por exemplo, se tiver saído da organização), poderá excluir a chave pública na instância e substituí-la por uma nova.

As chaves públicas estão localizadas no arquivo .ssh/authorized\_keys na instância.

Para adicionar ou substituir um par de chaves, você deve poder se conectar à sua instância. Se você perdeu sua chave privada existente ou iniciou sua instância sem um par de chaves, não poderá se conectar à instância e, portanto, não poderá adicionar ou substituir um par de chaves. Se você perdeu sua chave privada, talvez seja possível recuperá-la. Para obter mais informações, consulte [Conectar-se à instância do Linux em caso de perda da chave privada \(p. 1220\)](#). Se você iniciou sua instância sem um par de chaves, não conseguirá se conectar à instância a menos que escolha uma AMI configurada para permitir aos usuários outra maneira de efetuar login.

### Note

Esses procedimentos são para modificar o par de chaves para a conta do usuário padrão, como ec2-user. Para obter informações sobre como adicionar contas de usuário à sua instância, consulte [Gerenciar contas de usuário na instância do Amazon Linux \(p. 602\)](#).

Para adicionar ou substituir um par de chaves

1. Crie um par de chaves usando [o console do Amazon EC2 \(p. 1210\)](#) ou uma [ferramenta de terceiros \(p. 1212\)](#).
2. Recupere a chave pública do seu novo par de chaves. Para obter mais informações, consulte [Recuperar a chave pública da chave privada \(p. 1215\)](#).
3. [Conecte-se à sua instância \(p. 535\)](#) usando sua chave privada existente.

4. Usando um editor de texto à sua escolha, abra o arquivo `.ssh/authorized_keys` na instância. Cole as informações de chave pública do seu novo par de chaves abaixo das informações de chave pública existentes. Salve o arquivo.
5. Desconecte-se da sua instância e teste se você pode se conectar à sua instância usando novo arquivo de chave privada.
6. (Opcional) Se você estiver substituindo um par de chaves existente, conecte-se à sua instância e exclua as informações de chave pública para o par de chaves original do arquivo `.ssh/authorized_keys`.

#### Note

Se estiver usando um grupo do Auto Scaling, verifique se o par de chaves que você está substituindo não está especificado em seu modelo de execução ou em sua 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 [Modelos de execução](#) no Manual do usuário do Amazon EC2 Auto Scaling.

## 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 \(p. 1212\)](#) 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`).

#### Note

Para excluir a chave pública de uma instância, consulte [Excluir uma chave pública de uma instância \(p. 1220\)](#).

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.

## Excluir uma chave pública de uma instância

Se você criar uma AMI do Linux a partir de uma instância, as informações de chave pública serão copiadas da instância para a AMI. Se você executar uma instância da AMI, a nova instância incluirá a chave pública da instância original. Para impedir que alguém com a chave privada se conecte à nova instância, exclua a chave pública da instância original antes de criar a AMI.

### Para excluir uma chave pública de uma instância

1. [Conecte-se à sua instância \(p. 535\)](#).
2. Usando um editor de texto à sua escolha, abra o arquivo `.ssh/authorized_keys` na instância. Exclua as informações da chave pública e salve o arquivo.

### Warning

Depois de excluir a chave pública da instância e desconectar da instância, você não poderá se conectar a ela novamente, a menos que a AMI forneça outra maneira de fazer login.

## Conectar-se à instância do Linux em caso de perda da chave privada

Se você perder a chave privada de uma instância com EBS, poderá recobrar o acesso à sua instância. É necessário parar a instância, separar seu volume raiz e associá-lo a outra instância como um volume de dados, modificar o arquivo `authorized_keys` com uma nova chave pública, mover o volume de volta para a instância original e reiniciar a instância. Para obter mais informações sobre executar, conectar e parar instâncias, consulte [Ciclo de vida da instância \(p. 503\)](#).

Este procedimento é compatível apenas com instâncias com volumes raiz do EBS. Se o dispositivo raiz for um volume de armazenamento de instâncias, você não poderá usar esse procedimento para recuperar o acesso à instância. É necessário ter a chave privada para se conectar à instância. Para determinar o tipo de dispositivo raiz da sua instância, abra o console do Amazon EC2, escolha Instâncias, selecione a instância e verifique o valor de Tipo de dispositivo raiz no painel de detalhes. O valor é `ebs` ou `instance store`.

Além das etapas a seguir, há outras formas de se conectar à instância do Linux em caso de perda da chave privada. Para obter mais informações, consulte [Como posso me conectar à instância do Amazon EC2 se tiver perdido meu par de chaves SSH após o lançamento inicial?](#)

Etapas para se conectar a uma instância com EBS com um par de chaves diferente

- [Etapa 1: Criar um novo par de chaves \(p. 1221\)](#)
- [Etapa 2: Obter informações sobre a instância original e seu volume raiz \(p. 1221\)](#)
- [Etapa 3: Interromper a instância original \(p. 1221\)](#)
- [Etapa 4: Executar uma instância temporária \(p. 1221\)](#)
- [Etapa 5: Separar o volume raiz da instância original e associá-lo à instância temporária \(p. 1222\)](#)
- [Etapa 6: Adicionar a nova chave pública `authorized\_keys` no volume original montado à instância temporária \(p. 1222\)](#)

- [Etapa 7: Desmontar e separar o volume original da instância temporária e associá-lo novamente à instância original \(p. 1224\)](#)
- [Etapa 8: Conectar-se à instância original usando o novo par de chaves \(p. 1224\)](#)
- [Etapa 9: Limpeza \(p. 1224\)](#)

## Etapa 1: Criar um novo par de chaves

Crie um novo par de chaves usando o console do Amazon EC2 ou uma ferramenta de terceiros. Se você quiser nomear seu novo par de chaves exatamente igual ao par de chaves privadas perdido, primeiro exclua o par de chaves existente. Para obter mais informações sobre como criar um par de chaves, consulte [Criar um par de chaves usando o Amazon EC2 \(p. 1210\)](#) ou [Criar um par de chaves usando uma ferramenta de terceiros e importe a chave pública para o Amazon EC2 \(p. 1212\)](#).

## Etapa 2: Obter informações sobre a instância original e seu volume raiz

Anote as seguintes informações, porque elas serão necessárias para a conclusão deste procedimento.

Como obter informações sobre a instância original

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. Escolha Instâncias no painel de navegação e selecione a instância à qual você deseja se conectar. (Nós a chamamos de instância original.)
3. Na guia Details (Detalhes), anote o ID da instância e a ID da AMI.
4. Na guia Networking (Redes), anote a zona de disponibilidade.
5. Na guia Storage (Armazenamento), em Root device name (Nome do dispositivo raiz), anote o nome do dispositivo para o volume raiz (por exemplo, /dev/xvda). Em seguida, em Block devices (Dispositivos de bloco), encontre este nome do dispositivo e anote o ID do volume (por exemplo, vol-0a1234b5678c910de).

## Etapa 3: Interromper a instância original

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.

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.

## Etapa 4: Executar uma instância temporária

Escolha Launch Instance (Executar instância) e use o assistente de execução para executar uma instância temporária com as seguintes opções:

- Na página Escolha uma AMI, selecione a mesma AMI usada para executar a instância original. Se essa AMI estiver indisponível, você poderá criar uma AMI que pode usar a partir da instância interrompida. Para obter mais informações, consulte [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#).
- Na página Escolher um tipo de instância, deixe o tipo de instância padrão que o assistente seleciona para você.

- Na página Configure Instance Details (Configurar detalhes da instância) especifique a mesma zona de disponibilidade que a instância original. Se você estiver executando uma instância em uma VPC, selecione uma sub-rede nesta zona de disponibilidade.
- Na página Adicionar tags, adicione a tag Name=Temporary à instância para indicar que isso é uma instância temporária.
- Na página Revisar, escolha Iniciar. Escolha o par de chaves criado na Etapa 1 e selecione Iniciar instâncias.

## Etapa 5: Separar o volume raiz da instância original e associá-lo à instância temporária

1. No painel de navegação, selecione Volumes e selecione o volume do dispositivo raiz da instância original (você anotou o ID do volume em uma etapa anterior). Escolha Actions (Ações), Detach Volume (Desanexar volume) e Yes, Detach (Sim, desanexar). Espere o estado do volume tornar-se available. (Você pode precisar escolher o ícone Atualizar.)
2. Com o volume ainda selecionado, escolha Ações e, em seguida, Associar volume. Selecione o ID da instância temporária, anote o nome do dispositivo especificado em Device (Dispositivo) (por exemplo, /dev/sdf) e selecione Attach (Anexar).

### Note

Se você tiver executado a instância original a partir de uma AMI de AWS Marketplace e seu volume contiver códigos de AWS Marketplace , você deverá primeiro parar a instância temporária antes de associar o volume.

## Etapa 6: Adicionar a nova chave pública `authorized_keys` no volume original montado à instância temporária

1. Conecte-se à instância temporária.
2. Na instância temporária, monte o volume que você associou à instância de forma que possa acessar seu sistema de arquivos. Por exemplo, se o nome do dispositivo for /dev/sdf, use os comandos a seguir para montar o volume como /mnt/tempvol.

### Note

O nome de dispositivo pode aparecer de forma diferente em sua instância. Por exemplo, dispositivos montados como /dev/sdf podem ser exibidos como /dev/xvdf na instância. Algumas versões do Red Hat (ou suas variantes, como o CentOS) podem até mesmo incrementar a letra final com 4 caracteres, em que /dev/sdf torna-se /dev/xvdk.

- a. Use o comando lsblk determinar se o volume é particionado.

```
[ec2-user ~]$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda   202:0    0   8G  0 disk
##xvda1 202:1    0   8G  0 part /
xvdf   202:80   0 101G  0 disk
##xvdf1 202:81   0 101G  0 part
xvdg   202:96   0   30G  0 disk
```

No exemplo acima, /dev/xvda e /dev/xvdf são volumes particionados, e /dev/xvdg não é. Se seu volume estiver particionado, você montará a partição (/dev/xvdf1) em vez do dispositivo raw (/dev/xvdf) nas próximas etapas.

- b. Crie um diretório temporário para montar o volume.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

- c. Monte o volume (ou a partição) no ponto de montagem temporário usando o nome do volume ou do dispositivo identificado anteriormente. O comando necessário depende do sistema de arquivos do sistema operacional. Observe que o nome de dispositivo pode aparecer de forma diferente em sua instância. Consulte [note](#) nesta seção para obter mais informações.
- Amazon Linux, Ubuntu e Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 e RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

#### Note

Se você receber um erro informando que o sistema de arquivos está corrompido, execute o seguinte comando para usar o utilitário fsck para verificar o sistema de arquivos e reparar quaisquer problemas:

```
[ec2-user ~]$ sudo fsck /dev/xvdf1
```

3. Pela instância temporária, use o comando a seguir para atualizar `authorized_keys` no volume montado com a nova chave pública nova de `authorized_keys` para a instância temporária.

#### Important

Os exemplos a seguir usam o nome de usuário do Amazon Linux `ec2-user`. Você pode precisar substituir um nome de usuário diferente, como `ubuntu` para instâncias Ubuntu.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Se essa cópia tiver sido bem-sucedida, você poderá passar para a próxima etapa.

(Opcional) Caso contrário, se você não tiver permissão para editar arquivos em `/mnt/tempvol`, será necessário atualizar o arquivo usando `sudo` e conferir as permissões no arquivo para verificar se você pode fazer login na instância original. Use o comando a seguir para verificar as permissões no arquivo:

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw----- 1 222 500 398 Sep 13 22:54 authorized_keys
```

Nesta saída de exemplo, `222` é o ID do usuário e `500` é o ID do grupo. Em seguida, use `sudo` para executar novamente o comando de cópia que falhou.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Execute o comando a seguir novamente para determinar se as permissões foram alteradas.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

---

Se o ID do usuário e do grupo tiverem sido alterados, use o comando a seguir para restaurá-los.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

## Etapa 7: Desmontar e separar o volume original da instância temporária e associá-lo novamente à instância original

1. Na instância temporária, desmonte o volume que você associou para que possa reassociá-lo à instância original. Por exemplo, use o comando a seguir para desmontar o volume em /mnt/tempvol.

```
[ec2-user ~]$ sudo umount /mnt/tempvol
```

2. Desassocie o volume da instância temporária (você o desmontou na etapa anterior): no console do Amazon EC2, selecione o volume do dispositivo raiz da instância original (você anotou o ID do volume em uma etapa anterior), escolha Actions (Ações), Detach Volume (Desassociar volume) e, depois, selecione Yes, Detach (Sim, desassociar). Espere o estado do volume tornar-se available. (Você pode precisar escolher o ícone Atualizar.)
3. Associe o volume novamente à instância original: com o volume ainda selecionado, escolha Actions (Ações), Attach Volume (Associar volume). Selecione o ID da instância original, especifique o nome do dispositivo anotado anteriormente na [Etapa 2 \(p. 1221\)](#) para o anexo do dispositivo raiz original (/dev/sda1 ou /dev/xvda) e selecione Anexar.

### Important

Se você não especificar o mesmo nome do dispositivo do anexo original, não poderá iniciar a instância original. O Amazon EC2 espera que o volume raiz seja sda1 ou /dev/xvda.

## Etapa 8: Conectar-se à instância original usando o novo par de chaves

Selecione a instância original e escolha Instance state (Estado da instância) e Start instance (Iniciar instância). Após a instância entrar no estado running, você pode se conectar a ela usando o arquivo de chave privada do seu novo par de chaves.

### Note

Se o nome do novo par de chaves e do arquivo de chaves privadas correspondente for diferente do nome do par de chaves original, especifique o nome do novo arquivo de chave privada conectado à sua instância.

## Etapa 9: Limpeza

(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).

# Grupos de segurança do Amazon EC2 para instâncias do Linux

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 \(p. 1006\)](#).

A segurança é uma responsabilidade compartilhada entre a AWS e você. Para obter mais informações, consulte [Segurança no Amazon EC2 \(p. 1130\)](#). 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 Windows, consulte [Grupos de segurança do Amazon EC2 para instâncias do Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## Sumário

- [Regras de grupos de segurança \(p. 1226\)](#)
- [Rastreamento de conexão do grupo de segurança \(p. 1227\)](#)
  - [Conexões não rastreadas \(p. 1228\)](#)
  - [Example \(p. 1228\)](#)
  - [Throttling \(p. 1229\)](#)
- [Grupos de segurança padrão e personalizados \(p. 1229\)](#)
  - [Grupos de segurança padrão \(p. 1229\)](#)
  - [Os security groups personalizados \(p. 1230\)](#)
- [Trabalhar com grupos de segurança \(p. 1230\)](#)
  - [Crie um grupo de segurança \(p. 1231\)](#)
  - [Copiar um grupo de segurança \(p. 1232\)](#)
  - [Visualizar seus grupos de segurança \(p. 1233\)](#)
  - [Adicionar regras a um grupo de segurança \(p. 1233\)](#)
  - [Atualizar regras do grupo de segurança \(p. 1236\)](#)
  - [Excluir regras de um grupo de segurança \(p. 1238\)](#)
  - [Excluir um security group \(p. 1239\)](#)
  - [Atribuir um grupo de segurança a uma instância \(p. 1239\)](#)
  - [Para mudar o grupo de segurança de uma instância \(p. 1239\)](#)

- [Regras de grupo de segurança para diferentes casos de uso \(p. 1240\)](#)

- Regras do servidor da Web (p. 1241)
- Regras do servidor de banco de dados (p. 1241)
- Regras para conectar-se a instâncias pelo computador (p. 1242)
- Regras para conectar-se a instâncias por uma instâncias com o mesmo grupo de segurança (p. 1243)
- Regras de ping/ICMP (p. 1243)
- Regras do servidor DNS (p. 1244)
- Regras do Amazon EFS (p. 1244)
- Regras do Elastic Load Balancing (p. 1244)
- Regras de emparelhamento de VPC (p. 1245)

## 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 \(p. 1566\)](#).
- 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 \(p. 1227\)](#).
- 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 \(p. 1227\)](#).

- 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 \(p. 937\)](#). 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 22 (SSH) do endereço IP 203.0.113.1 e outra regra que permita acesso à porta TCP 22 de todos, todos terão acesso à porta TCP 22.

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 \(p. 1032\)](#).

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平衡ador de carga ou o tamanho das instâncias registradas com o平衡ador 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 \(p. 1229\)](#)
- [Os security groups personalizados \(p. 1230\)](#)

## 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 \(p. 1240\)](#).

## 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 \(p. 1239\)](#).

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 \(p. 1239\)](#).

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 \(p. 1231\)](#)
- [Copiar um grupo de segurança \(p. 1232\)](#)
- [Visualizar seus grupos de segurança \(p. 1233\)](#)
- [Adicionar regras a um grupo de segurança \(p. 1233\)](#)
- [Atualizar regras do grupo de segurança \(p. 1236\)](#)
- [Excluir regras de um grupo de segurança \(p. 1238\)](#)
- [Excluir um security group \(p. 1239\)](#)
- [Atribuir um grupo de segurança a uma instância \(p. 1239\)](#)
- [Para mudar o grupo de segurança de uma instância \(p. 1239\)](#)

## 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 \(p. 1233\)](#).
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 \(p. 1233\)](#).

## 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 \(p. 1551\)](#).

## 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 \(p. 1240\)](#) e [Regras de grupos de segurança \(p. 1226\)](#).

## 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.
- 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 fornecer 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.

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 saída somente do endereço IPv4 público do computador local.
- 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 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 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 \(p. 1240\)](#).

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.

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 \(p. 516\)](#).
- Para especificar um grupo de segurança em um modelo de execução, consulte Etapa 6 de [Criar um novo modelo de execução usando parâmetros definidos \(p. 519\)](#).

## 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. 1241)

- [Regras do servidor de banco de dados \(p. 1241\)](#)
- [Regras para conectar-se a instâncias pelo computador \(p. 1242\)](#)
- [Regras para conectar-se a instâncias por uma instâncias com o mesmo grupo de segurança \(p. 1243\)](#)
- [Regras de ping/ICMP \(p. 1243\)](#)
- [Regras do servidor DNS \(p. 1244\)](#)
- [Regras do Amazon EFS \(p. 1244\)](#)
- [Regras do Elastic Load Balancing \(p. 1244\)](#)
- [Regras de emparelhamento de VPC \(p. 1245\)](#)

## 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
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

Tipo de protocolo	Número do protocolo	Porta	Observações
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
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

Tipo de protocolo	Número do protocolo	Porta	IP de origem
			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 (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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Regras de grupo de segurança para diferentes casos de uso

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.
<b>Saída</b>				
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.

<b>Entrada</b>				
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 flua 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 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.

## 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.

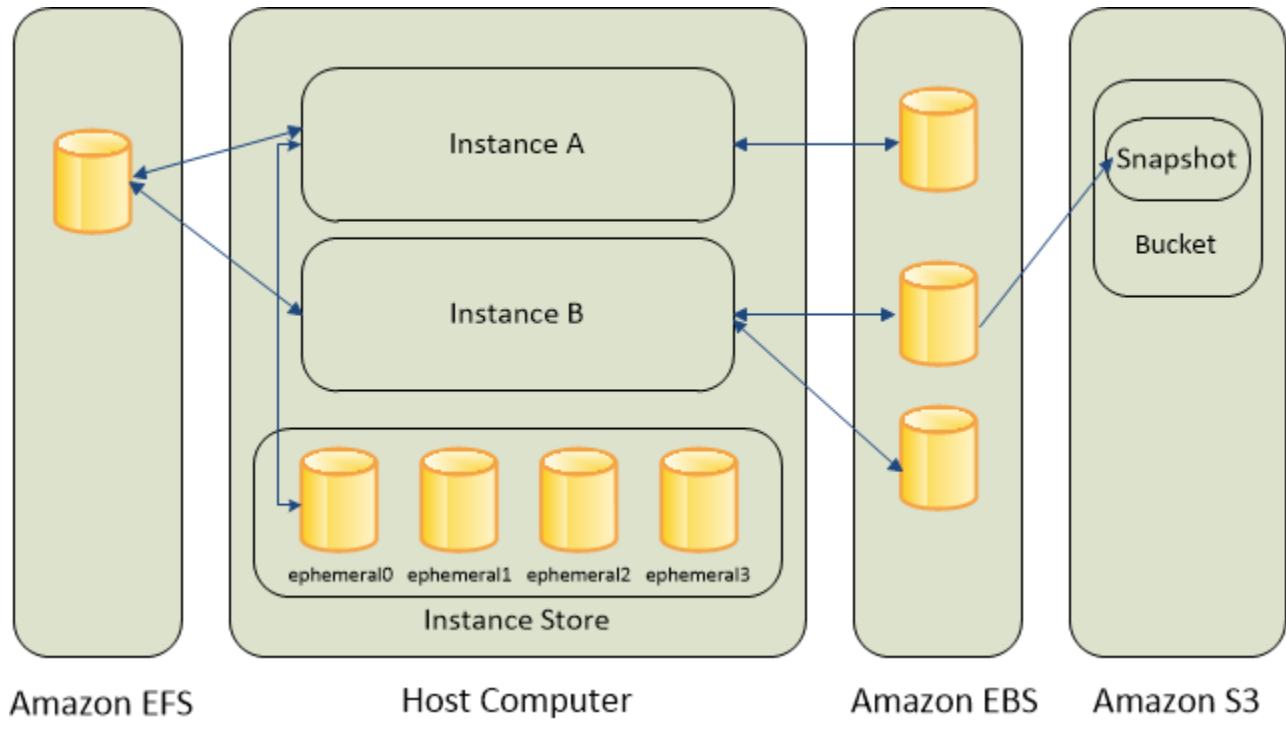
# Storage

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 \(p. 1248\)](#)
- [Armazenamento de instâncias do Amazon EC2 \(p. 1494\)](#)
- [Usar o Amazon EFS com o Amazon EC2 \(p. 1515\)](#)
- [Usar o Amazon S3 com a Amazon EC2 \(p. 1514\)](#)

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 \(p. 1418\)](#).

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 \(p. 1248\)](#).

#### 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 \(p. 1494\)](#).

#### Sistema de arquivos do Amazon EFS

O Amazon EFS fornece armazenamento de arquivos escalável para uso com o Amazon EC2. Você pode criar um sistema de arquivos de EFS e configurar suas instâncias para montar o sistema de arquivos. Você pode usar um sistema de arquivos de EFS como uma fonte de dados comum para workloads e aplicações em execução em várias instâncias. Para obter mais informações, consulte [Usar o Amazon EFS com o Amazon EC2 \(p. 1515\)](#).

#### 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 \(p. 1514\)](#).

#### 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 \(p. 1530\)](#).

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 \(p. 1277\)](#).

#### 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 \(p. 1249\)](#)
- [Volumes do Amazon EBS \(p. 1250\)](#)
- [Screencasts do Amazon EBS \(p. 1303\)](#)
- [Amazon Data Lifecycle Manager \(p. 1359\)](#)
- [Serviços de dados do Amazon EBS \(p. 1405\)](#)
- [Amazon EBS e NVMe em instâncias Linux \(p. 1434\)](#)
- [Instâncias otimizadas para Amazon EBS \(p. 1438\)](#)
- [Performance de volume do Amazon EBS em instâncias Linux \(p. 1460\)](#)
- [Métricas do Amazon CloudWatch para o Amazon EBS \(p. 1477\)](#)
- [Amazon CloudWatch Events para Amazon EBS \(p. 1484\)](#)
- [Cotas do Amazon EBS \(p. 1494\)](#)

## 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 \(p. 1253\)](#).

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 \(p. 1418\)](#).
- 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 \(p. 1303\)](#).
- 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 Linux \(p. 1460\)](#).

## 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. Dependendo do volume e dos tipos de instância, você pode usar a opção [Multi-Attach \(Vinculação múltipla\) \(p. 1278\)](#) para montar um volume para várias instâncias ao mesmo tempo.

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 \(p. 1253\)](#).

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 \(p. 1565\)](#).

Para obter mais informações sobre definição de preço, consulte [Definição de preço do Amazon EBS](#).

#### Tópicos

- [Benefícios de usar volumes do EBS \(p. 1251\)](#)
- [Tipos de volume do Amazon EBS \(p. 1253\)](#)
- [Restrições de tamanho e configuração de um volume do EBS \(p. 1271\)](#)
- [Crie um volume do Amazon EBS. \(p. 1274\)](#)
- [Vincular um volume de Amazon EBS a uma instância \(p. 1277\)](#)
- [Anexar um volume a várias instâncias com o Multi-Attach do Amazon EBS \(p. 1278\)](#)
- [Disponibilizar um volume do Amazon EBS para uso no Linux \(p. 1283\)](#)
- [Visualizar informações sobre um volume do Amazon EBS \(p. 1287\)](#)
- [Substituir um volume do Amazon EBS \(p. 1288\)](#)
- [Monitorar o status de seus volumes \(p. 1292\)](#)
- [Desanexar um volume do Amazon EBS de uma instância Linux \(p. 1300\)](#)
- [Excluir um volume de Amazon EBS \(p. 1302\)](#)

## 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 ext3, 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.

É possível anexar volumes do EBS io1 e io2 para até 16 instâncias baseadas em Nitro. Para obter mais informações, consulte [Anexar um volume a várias instâncias com o Multi-Attach do Amazon EBS \(p. 1278\)](#). Caso contrário, é possível anexar um volume do EBS a uma única instância.

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 \(p. 1477\)](#). Para obter informações sobre como acompanhar o status de seus volumes, consulte [Amazon CloudWatch Events para Amazon EBS \(p. 1484\)](#).

### 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 \(p. 1418\)](#).

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 permita 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 de Amazon EBS \(p. 1418\)](#).

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 \(p. 1552\)](#).

Para fazer backup de seus volumes automaticamente, é possível usar [Amazon Data Lifecycle Manager \(p. 1359\)](#) 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 \(p. 1405\)](#).

## 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 \(SSD\) \(p. 1253\)](#) — 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 \(HDD\) \(p. 1255\)](#): otimizadas para grandes workloads de transmissão em que o atributo de performance dominante é a taxa de transferência.
- [Geração anterior \(p. 1256\)](#) — 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 \(p. 1438\)](#). Para obter mais informações sobre como aproveitar ao máximo seus volumes do EBS, consulte [Performance de volume do Amazon EBS em instâncias Linux \(p. 1460\)](#).

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 \(p. 1438\)](#).

	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"> <li>Aplicações interativas de baixa latência</li> <li>Ambientes de teste e desenvolvimento</li> </ul>		Workloads que exigem: <ul style="list-style-type: none"> <li>Latência média abaixo de um milissegundo</li> <li>Performance estável de IOPS</li> <li>Mais de 64.000 IOPS ou 1.000 MiB/s de taxa de transferência</li> </ul>	<ul style="list-style-type: none"> <li>Workloads que exigem performance de IOPS sustentado ou mais do que 16.000 IOPS</li> <li>Workloads de banco de dados com alto consumo de E/S</li> </ul>			
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 \(p. 1405\)](#).

† O número máximo de IOPS e a taxa de transferência são garantidos somente em [Instâncias criadas no Sistema Nitro \(p. 210\)](#) 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 \(p. 1405\)](#).

‡ 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 \(p. 1262\)](#).

## 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 \(p. 1438\)](#).

	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"><li>• Big data</li><li>• Data warehouses</li><li>• Processamento de logs</li></ul>	<ul style="list-style-type: none"><li>• Armazenamento orientado para taxa de transferência para dados acessados raramente</li><li>• Cenários nos quais o menor custo de armazenamento é importante</li></ul>
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

	HDD otimizado para taxa de transferência	Disco rígido frio
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
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

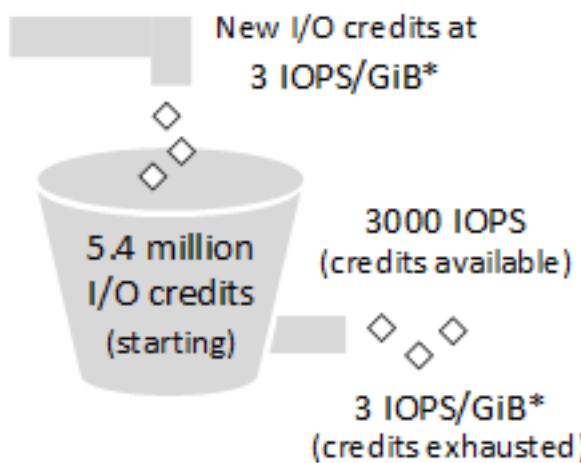
## Volumes de Finalidade geral (SSD) (gp2)

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

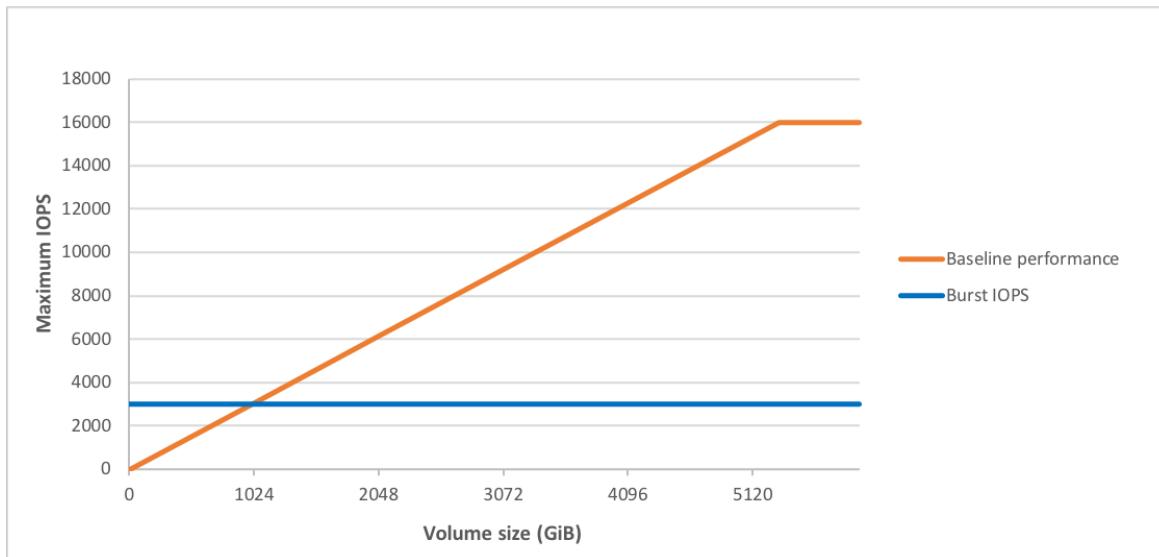
A performance dos volumes de gp2 é vinculada ao tamanho do volume, que determina o nível de performance basal do volume e a rapidez com que acumula créditos de E/S; volumes maiores têm níveis de performance basais mais altos e acumulam créditos de E/S com maior rapidez. Os créditos de E/S representam 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. 210), 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

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
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 \(p. 1463\)](#).

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 de bucket de intermitência, consulte [Monitorar o saldo de bucket de intermitência para volumes \(p. 1271\)](#).

### 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:

$$V = \frac{T}{IR}$$

```
    250 MiB/s
= -----
(256 KiB)(3 IOPS/GiB)

    [(250)(2^20)(Bytes)]/s
= -----
(256)(2^10)(Bytes)([3 IOP/s]/[(2^30)(Bytes)]) 

    (250)(2^20)(2^30)(Bytes)
= -----
(256)(2^10)(3)

= 357,913,941,333 Bytes

= 333# GiB (334 GiB in practice because volumes are provisioned in whole gibibytes)
```

## 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 \(p. 1262\)](#), 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 \(p. 1262\)](#) 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 \(p. 1262\)](#), 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 \(p. 1262\)](#).
  - 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 \(p. 1262\)](#), o volume não será executado automaticamente no Block Express.

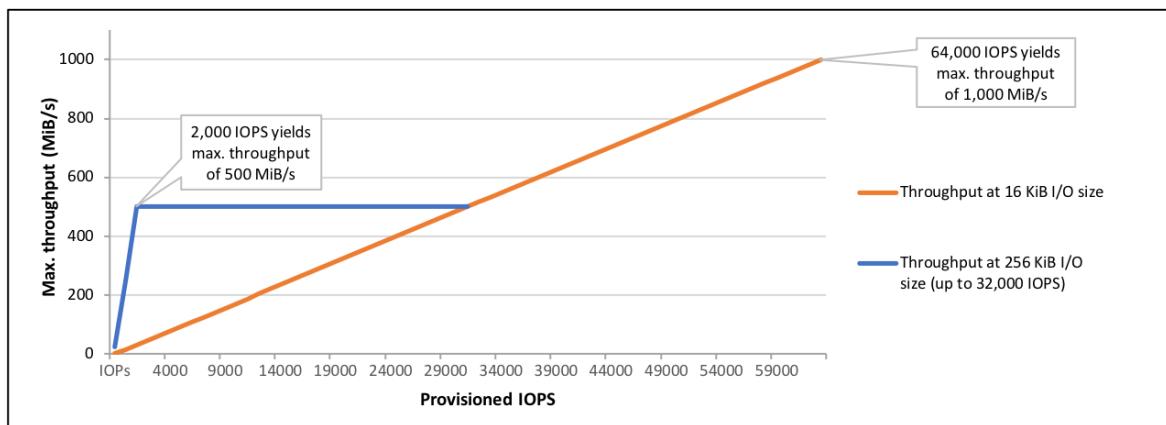
- Não é possível iniciar um volume `io2` criptografado que tem tamanho superior a 16 TiB ou IOPS superior a 64.000 de um snapshot não criptografado ou de um snapshot criptografado compartilhado. Nesse caso, você deve primeiro criar um snapshot criptografado em sua conta e depois usar esse snapshot para 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 \(p. 1262\)](#). 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 \(p. 1262\)](#).
  - 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 \(p. 1262\)](#), o volume não será mais executado no Block Express e fornecerá latência `io2`.
- Lembre-se do seguinte aomodificar 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 \(p. 1262\)](#).
  - 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 \(p. 210\)](#). 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 \(p. 1262\)](#)
- [Performance \(p. 1263\)](#)
- [Quotas \(p. 1263\)](#)
- [Definição de preço e faturamento \(p. 1263\)](#)

## 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-`

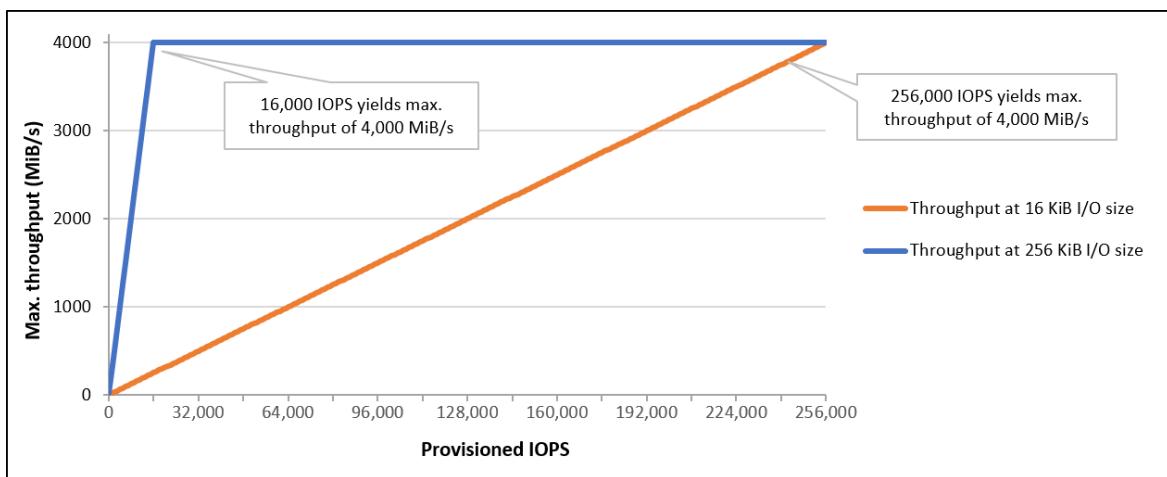
`northeast-1` e `eu-central-1`. A disponibilidade da instância R5b pode variar de acordo com a zona de disponibilidade. Para obter mais informações sobre a disponibilidade do R5b, consulte [Localizar um tipo de instância do Amazon EC2](#).

- 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 [Iniciar volumes de Amazon EBS \(p. 1466\)](#).

## 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.

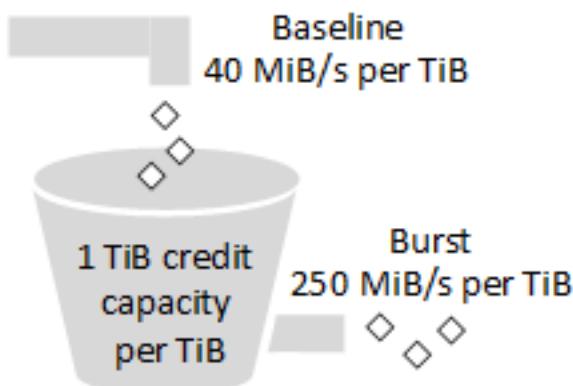
Esse tipo de volume é otimizado para workloads que envolvem E/S sequencial e grande, e recomendamos que clientes com workloads executando E/S pequena e aleatória usem gp2. Para obter mais informações, consulte [Ineficiência de pequenas leituras/escritas no HDD \(p. 1271\)](#).

#### 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.

### ST1 burst bucket



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:

$$12.5 \text{ TiB} \times \frac{40 \text{ MiB/s}}{1 \text{ TiB}} = 500 \text{ MiB/s}$$

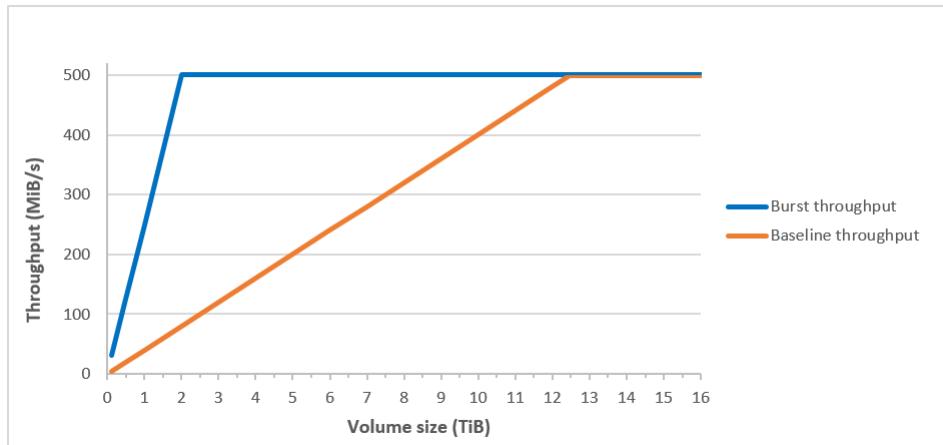
A taxa de transferência varia de 31 MiB/s a um limite de 500 MiB/s, que é alcançado em 2 TiB, da seguinte forma:

$$\frac{250 \text{ MiB/s}}{2 \text{ TiB} \times \frac{1}{1 \text{ TiB}}} = 500 \text{ MiB/s}$$

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 \(p. 1271\)](#).

## 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.

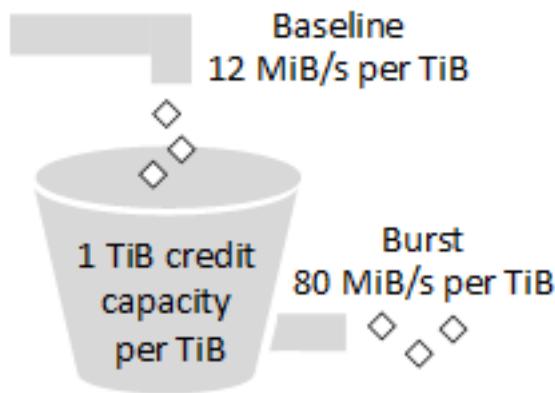
#### Note

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 \(p. 1271\)](#).

## 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 altas. 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:

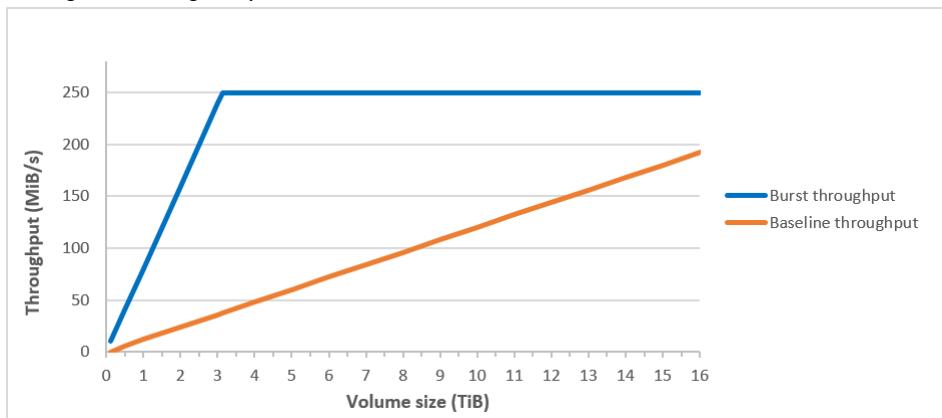
$$80 \text{ MiB/s} \\ 3.125 \text{ TiB} \times \frac{80 \text{ MiB/s}}{1 \text{ TiB}} = 250 \text{ MiB/s}$$

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 \(p. 1271\)](#).

## 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 \(p. 1271\)](#).

## 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 \(p. 1438\)](#).

## 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 \(p. 1463\)](#). 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 \(p. 1271\)](#)
- [Limitações do serviço \(p. 1272\)](#)
- [Esquemas de particionamento \(p. 1272\)](#)
- [Tamanhos de blocos de dados \(p. 1273\)](#)

## 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	$2^{32}$ <sup>32</sup>	2 TiB	2 TiB	2 TiB	2 TiB	2 TiB
GPT	$2^{64}$	64 ZiB	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](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 \(p. 1262\)](#).

## 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.
- Os volumes de inicialização do Linux podem usar o esquema de particionamento MBR ou GPT. O MBR oferece suporte a volumes de até 2047 GiB (2 TiB - 1 GiB). O GPT com GRUB 2 oferece suporte a volumes de inicialização de 2 TiB ou maiores. Se a AMI do Linux usar MBR, o volume de inicialização será limitado a 2.047 GiB, mas os volumes de não inicialização não terão esse limite. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Linux \(p. 1283\)](#).

## 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 \(p. 1273\)](#). 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

Tamanho de bloco	Tamanho máx. do volume
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 \(p. 1420\)](#).

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 \(p. 1438\)](#).

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 \(p. 1466\)](#).

### 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. \(p. 510\)](#) e [Mapeamentos de dispositivos de blocos \(p. 1530\)](#).
- Crie um volume do EBS e anexe-o a uma instância em execução. Para obter mais informações, consulte [Criar um volume vazio \(p. 1274\)](#) 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 \(p. 1275\)](#) 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 \(p. 1542\)](#).
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 \(p. 1253\)](#).
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 \(p. 1271\)](#).
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 \(p. 1418\)](#).
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 \(p. 1552\)](#).
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 \(p. 1277\)](#).

## 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 [Inicializar volumes de Amazon EBS \(p. 1466\)](#).

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 \(p. 1420\)](#).

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. \(p. 1313\)](#).

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 \(p. 1253\)](#).
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 \(p. 1421\)](#) 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 \(p. 1271\)](#).

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 iopol2.
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 \(p. 1277\)](#).

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 \(p. 1405\)](#).

#### 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 \(p. 1536\)](#).

#### Prerequisites

- Determine quantos volumes você pode associar à sua instância. Para obter mais informações, consulte [Limites de volumes de instância \(p. 1520\)](#).
- Determine se você pode anexar seu volume a várias instâncias e habilite a opção Anexar várias. Para obter mais informações, consulte [Anexar um volume a várias instâncias com o Multi-Attach do Amazon EBS \(p. 1278\)](#).
- 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 \(p. 1420\)](#).
- 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 Linux. \(p. 1528\)](#).
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 Linux \(p. 1283\)](#).

#### 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](#).

## Anexar um volume a várias instâncias com o Multi-Attach do Amazon EBS

O Amazon EBS Multi-Attach permite que você anexe um único volume SSD de IOPS provisionadas (io1 ou io2) a várias instâncias na mesma zona de disponibilidade. Você pode anexar vários volumes habilitados para Multi-Attach a uma instância ou conjunto de instâncias. Cada instância à qual o volume está anexado tem permissão completa de leitura e gravação no volume compartilhado. O Multi-Attach facilita obter maior disponibilidade da aplicação em aplicações Linux clusterizadas que gerenciam operações de gravação simultâneas.

#### Tópicos

- [Considerações e limitações \(p. 337\)](#)
- [Performance \(p. 1279\)](#)
- [Como trabalhar com Multi-Attach \(p. 1280\)](#)
- [Monitorar um volume habilitado para Multi-Attach \(p. 1283\)](#)
- [Definição de preço e faturamento \(p. 1283\)](#)

## Considerações e limitações

- Os volumes habilitados para vinculação múltipla podem ser anexados a até 16 instâncias do Linux criadas no [Sistema Nitro \(p. 210\)](#) que estejam na mesma zona de disponibilidade. Você pode anexar um volume Multi-Attach a várias instâncias do Windows, mas o sistema operacional não reconhece os dados no volume compartilhado entre as instâncias, o que pode resultar em inconsistência de dados.

- O Multi-Attach é suportado exclusivamente em [Volumes de Provisioned IOPS SSD \(p. 1260\)](#).
  - O Multi-Attach para volumes de `io1` está disponível somente nas seguintes Regiões: `us-east-1`, `us-west-2`, `eu-west-1` e `ap-northeast-2`.
- O Multi-Attach para volumes `io2` e `io1` do Block Express está disponível em todas as regiões com suporte para volumes desses tipos de volume.
- Os sistemas de arquivos padrão, como XFS e EXT4, não foram projetados para serem acessados simultaneamente por vários servidores, como as instâncias do EC2. O uso do Multi-Attach com um sistema de arquivos padrão pode resultar em dados corrompidos ou perdidos, portanto, não é seguro para workloads de produção. Você pode usar um sistema de arquivos em cluster para garantir a resiliência e a confiabilidade de dados para workloads de produção.
  - Volumes habilitados para Multi-Attach não são compatíveis com cercas de E/S. Os protocolos de cercas de E/S controlam o acesso de gravação em um ambiente de armazenamento compartilhado para manter a consistência dos dados. Suas aplicações devem fornecer uma ordem de gravação para as instâncias anexadas para manter a consistência dos dados.
  - Volumes habilitados para Multi-Attach não podem ser criados como volumes de inicialização.
  - Os volumes habilitados para Multi-Attach podem ser anexados a um mapeamento de dispositivo de bloco por instância.
  - O Multi-Attach não pode ser habilitado durante a execução da instância usando o console do Amazon EC2 ou a API RunInstances.
  - Os volumes habilitados para Multi-Attach que têm um problema na camada da infraestrutura do Amazon EBS não estão disponíveis para todas as instâncias anexadas. Problemas no Amazon EC2 ou na camada de rede podem afetar apenas algumas instâncias anexadas.
  - A tabela a seguir mostra o suporte a modificação de volumes para volumes `io1` e `io2` habilitados para Multi-Attach.

	<b>io2</b> Volumes do	<b>io1</b> Volumes do
Modificar tipo de volume	X	X
Modificar tamanho do volume	✓	X
Modificar as IOPS provisionadas	✓	X
Ativar Multi-Attach	✓ *	X
Desativar Multi-Attach	✓ *	X

\* Você não pode ativar ou desativar o Multi-Attach enquanto o volume estiver associado a uma instância.

## Performance

Cada instância anexada pode direcionar sua performance máxima de IOPS até a performance máxima provisionada do volume. No entanto, a performance agregada de todas as instâncias anexadas não pode exceder a performance máxima provisionada do volume. Se a demanda das instâncias anexadas por maior que as IOPS provisionadas do volume, o volume não excederá sua performance provisionada.

Por exemplo, digamos que você crie um volume habilitado para Multi-Attach de `io2` com 50,000 IOPS provisionadas e o anexe a uma instância `m5.8xlarge` e a uma instância `c5.12xlarge`. As instâncias `m5.8xlarge` e `c5.12xlarge` são compatíveis com um máximo de 30,000 e 40,000 IOPS

respectivamente. Cada instância pode direcionar seu máximo de IOPS, pois ele é menor do que as IOPS provisionadas do volume 50 , 000. No entanto, se as duas instâncias direcionarem a E/S para o volume simultaneamente, suas IOPS combinadas não poderão exceder a performance provisionada do volume de 50 , 000 IOPS. O volume não excederá 50 , 000 IOPS.

Para obter uma performance consistente, é uma prática recomendada equilibrar a E/S direcionada de instâncias anexadas entre os setores de um volume habilitado para Multi-Attach.

## Como trabalhar com Multi-Attach

Os volumes habilitados para Multi-Attach podem ser gerenciados da mesma maneira como você gerenciaria qualquer outro volume do Amazon EBS. No entanto, para usar a funcionalidade Multi-Attach, você deve habilitá-la para o volume. Quando um volume é criado, o Multi-Attach está desabilitado por padrão.

### Sumário

- [Ativar Multi-Attach \(p. 1280\)](#)
- [Desativar Multi-Attach \(p. 1281\)](#)
- [Anexar um volume a instâncias \(p. 1282\)](#)
- [Excluir no encerramento \(p. 1282\)](#)

### Ativar Multi-Attach

Você pode habilitar o Multi-Attach para volumes io1 e io2 durante a criação.

Use um dos seguintes métodos para habilitar o Multi-Attach para um volume de io1 ou de io2 durante a criação.

#### Console

##### Como habilitar o Multi-Attach durante a criação do volume

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Volumes.
3. Escolha Create Volume (Criar volume).
4. Para Volume Type (Tipo de volume), escolha Provisioned IOPS SSD (io1) (SSD de IOPS provisionadas (io1) ou Provisioned IOPS SSD (io2) (SSD provisionado de IOPS (io2)).
5. Em Size (Tamanho) e IOPS, escolha o tamanho necessário do volume e o número de IOPS a serem provisionadas.
6. Em Availability Zone (Zona de disponibilidade), escolha a mesma Zona de disponibilidade em que as instâncias se encontram.
7. Em Multi-Attach, escolha Enable (Habilitar).
8. Escolha Create Volume (Criar volume).

#### Command line

##### Como habilitar o Multi-Attach durante a criação do volume

Use o comando `create-volume` e especifique o parâmetro `--multi-attach-enabled`.

```
$ aws ec2 create-volume --volume-type io2 --multi-attach-enabled --size 100 --iops 2000  
--region us-west-2 --availability-zone us-west-2b
```

Você também pode habilitar o Multi-Attach para volumes de `io2` depois que eles foram criados.

#### Note

Você não pode habilitar o Multi-Attach para volumes de `io1` após a criação.

Use um dos métodos a seguir para habilitar o Multi-Attach para um volume do Amazon EBS depois que ele foi criado.

#### Console

Para ativar o Multi-Attach após a criação

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), Modify Volume (Modificar volume).
4. Em Multi-Attach, escolha Enable (Habilitar).
5. Selecione Modify.

#### Command line

Para ativar o Multi-Attach após a criação

Use o comando `modify-volume` e especifique o parâmetro `--multi-attach-enabled`.

```
$ aws ec2 modify-volume --volume-id vol-1234567890abcdef0 --multi-attach-enabled
```

## Desativar Multi-Attach

Você pode desativar o Multi-Attach para um volume de `io2` somente se ele estiver conectado a não mais do que uma instância.

#### Note

Não é possível desativar o Multi-Attach para volumes de `io1` após a criação.

Use um dos seguintes métodos para desativar o Multi-Attach para um volume de `io2`.

#### Console

Para desativar o Multi-Attach

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), Modify Volume (Modificar volume).
4. Para Multi-Attach, desmarque Enable (Ativar).
5. Selecione Modify.

#### Command line

Para desativar o Multi-Attach após a criação

Use o comando `modify-volume` e especifique o parâmetro `-no-multi-attach-enabled`.

```
$ aws ec2 modify-volume --volume-id vol-1234567890abcdef0 --no-multi-attach-enabled
```

## Anexar um volume a instâncias

Você anexa um volume habilitado para vinculação múltipla a uma instância da mesma maneira como anexa qualquer outro volume do EBS. Para obter mais informações, consulte [Vincular um volume de Amazon EBS a uma instância \(p. 1277\)](#).

## Excluir no encerramento

Os volumes habilitados para Multi-Attach serão excluídos no encerramento da instância se a última instância anexada for encerrada, e se essa instância estiver configurada para excluir o volume ao encerrar. Se o volume estiver anexado a várias instâncias que têm configurações diferentes de exclusão no encerramento em seus mapeamentos de dispositivos de blocos de volume, a configuração de mapeamento de dispositivo de blocos da última instância anexada determinará o comportamento da exclusão no encerramento.

Para garantir a exclusão previsível no comportamento de encerramento, habilite ou desabilite a exclusão no encerramento para todas as instâncias às quais o volume está anexado.

Por padrão, quando um volume é anexado a uma instância, a configuração de exclusão no encerramento do mapeamento de dispositivo de blocos é definida como falsa. Para habilitar a exclusão no encerramento para um volume habilitado para Multi-Attach, modifique o mapeamento de dispositivo de blocos.

Se desejar que o volume seja excluído quando as instâncias anexadas forem encerradas, habilite a exclusão no encerramento no mapeamento de dispositivo de blocos para todas as instâncias anexadas. Para reter o volume depois que as instâncias anexadas tiverem sido encerradas, desabilite a exclusão no encerramento no mapeamento de dispositivo de blocos para todas as instâncias anexadas. Para obter mais informações, consulte [Preservar volumes do Amazon EBS no encerramento da instância \(p. 591\)](#).

Você pode modificar a configuração de exclusão no encerramento de uma instância na execução ou depois que ela for executada. Se você habilitar ou desabilitar a exclusão no encerramento durante a execução da instância, as configurações se aplicarão somente aos volumes anexados na execução. Se você anexar um volume a uma instância após a execução, deverá definir explicitamente o comportamento de exclusão no encerramento para esse volume.

Você pode modificar a configuração de exclusão no encerramento de uma instância usando somente as ferramentas de linha de comando.

Como modificar a configuração de exclusão no encerramento de uma instância existente

Use o comando [modify-instance-attribute](#) e especifique o atributo DeleteOnTermination em --block-device-mappings option.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

Especifique o seguinte em mapping.json.

```
[  
  {  
    "DeviceName": "/dev/sdf",  
    "Ebs": {  
      "DeleteOnTermination": true/false  
    }  
  }  
]
```

[ ]

## Monitorar um volume habilitado para Multi-Attach

Você pode monitorar um volume habilitado para Multi-Attach usando as métricas do CloudWatch para volumes do Amazon EBS. Para obter mais informações, consulte [Métricas do Amazon CloudWatch para o Amazon EBS \(p. 1477\)](#).

Os dados são agregados em todas as instâncias anexadas. Você não pode monitorar métricas para instâncias anexadas individuais.

## Definição de preço e faturamento

Não há cobranças adicionais pelo uso do recurso Multi-Attach do Amazon EBS. Você receberá a cobrança dos encargos padrão aplicáveis aos volumes SSD de IOPS provisionadas (io1 e io2). Para obter mais informações, consulte [Definição de preço do Amazon EBS](#).

## Disponibilizar um volume do Amazon EBS para uso no Linux

Depois que você associar um volume do Amazon EBS à instância, ele será exposto como um dispositivo de blocos. 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.

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 \(p. 1303\)](#).

Você pode obter instruções sobre volumes em uma instância Windows em [Disponibilização de um volume para uso no Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## Formatar e montar um volume anexado

Suponha que você tenha uma instância do EC2 com um volume do EBS para o dispositivo raiz, /dev/xvda, e que tenha anexado um volume do EBS vazio à instância usando o /dev/sdf. Use o procedimento a seguir para disponibilizar o volume recém-anexado para uso.

Para formatar e montar um volume do EBS no Linux

1. Conecte-se à sua instância usando SSH. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. O dispositivo pode ser anexado à instância com um nome de dispositivo diferente do especificado no mapeamento de dispositivos de blocos. Para obter mais informações, consulte [Nomes de dispositivos em instâncias do Linux \(p. 1528\)](#). Use o comando lsblk para visualizar os dispositivos de disco disponíveis e seus pontos de montagem (se aplicável) para ajudá-lo a determinar o nome de dispositivo correto a usar. A saída de lsblk remove o prefixo /dev/ dos caminhos completos do dispositivo.

Veja a seguir um exemplo de saída para uma instância criada no [Sistema Nitro \(p. 210\)](#), que expõe os volumes do EBS como dispositivos de blocos NVMe. O dispositivo raiz é /dev/nvme0n1, que tem duas partições chamadas nvme0n1p1 e nvme0n1p128. O volume anexado é /dev/nvme1n1, que ainda não tem partições e não está montado.

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1    259:0    0  10G  0 disk
nvme0n1    259:1    0   8G  0 disk
```

```
-nvme0n1p1    259:2      0   8G  0 part /
-nvme0n1p128  259:3      0   1M  0 part
```

Este é um exemplo de saída de uma instância T2. O dispositivo raiz é /dev/xvda, que tem uma partição chamada xvda1. O volume anexado é /dev/xvdf, que ainda não tem partições e não está montado.

```
[ec2-user ~]$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda   202:0    0   8G  0 disk
-xvda1  202:1    0   8G  0 part /
xvdf   202:80   0  10G  0 disk
```

3. Determine se existe um sistema de arquivos no volume. Os novos volumes são dispositivos de blocos raw, e você deve criar um sistema de arquivos neles antes que possa montá-los e usá-los. Os volumes que foram criados de snapshots provavelmente já têm um sistema de arquivos neles. Se você criar um sistema de arquivos sobre o sistema de arquivos existente, a operação sobrescreverá seus dados.

Use um ou ambos os métodos a seguir para determinar se há um sistema de arquivos no volume:

- Use o comando file -s para obter informações sobre o dispositivo específico, como o tipo de sistema de arquivos. Se a saída mostrar simplesmente data, como no exemplo de saída a seguir, não há sistema de arquivos no dispositivo

```
[ec2-user ~]$ sudo file -s /dev/xvdf
/dev/xvdf: data
```

Se o dispositivo tiver um sistema de arquivos, o comando mostrará informações sobre o tipo de sistema de arquivos. Por exemplo, a saída a seguir mostra um dispositivo raiz com o sistema de arquivos XFS.

```
[ec2-user ~]$ sudo file -s /dev/xvda1
/dev/xvda1: SGI XFS filesystem data (blksz 4096, inosz 512, v2 dirs)
```

- Use o comando lsblk -f para obter informações sobre todos os dispositivos vinculados à instância.

```
[ec2-user ~]$ sudo lsblk -f
```

Por exemplo, a saída a seguir mostra que existem três dispositivos vinculados às instâncias —nvme1n1nvme0n1 e nvme2n1. A primeira coluna lista os dispositivos e suas partições. A coluna FSTYPE exibe o tipo de sistema de arquivos para cada dispositivo. Se a coluna estiver vazia para um dispositivo específico, isso significa que o dispositivo não possui um sistema de arquivos. Neste caso, o dispositivo nvme1n1 e as partições nvme0n1p1 no dispositivo nvme0n1 são formatados usando o sistema de arquivos XFS, enquanto o dispositivo nvme2n1 e as partições nvme0n1p128 no dispositivo nvme0n1 não têm sistemas de arquivos.

```
NAME   FSTYPE LABEL UUID           MOUNTPOINT
nvme1n1     xfs  7f939f28-6dcc-4315-8c42-6806080b94dd
nvme0n1
##nvme0n1p1 xfs   / 90e29211-2de8-4967-b0fb-16f51a6e464c      /
##nvme0n1p128
nvme2n1
```

Se a saída destes comandos mostrar que não há nenhum sistema de arquivos no dispositivo, você deverá criar um.

4. (Condicional) Se você descobriu que há um sistema de arquivos no dispositivo na etapa anterior, ignore esta etapa. Se você tiver um volume vazio, use o comando mkfs -t para criar um sistema de arquivos no volume.

**Warning**

Não use esse comando se você estiver montando um volume que já contenha dados (por exemplo, um volume que foi criado de um snapshot). Caso contrário, você formatará o volume e excluirá os dados existentes.

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/xvdf
```

Se você receber um erro de que `mkfs.xfs` não foi encontrado, use o seguinte comando para instalar as ferramentas do XFS e repita o comando anterior:

```
[ec2-user ~]$ sudo yum install xfsprogs
```

5. Use o comando mkdir para criar um diretório de ponto de montagem para o volume. O ponto de montagem é o local onde o volume está localizado na árvore do sistema de arquivos e onde você lê e grava arquivos depois de montar o volume. O exemplo a seguir cria um diretório denominado `/data`.

```
[ec2-user ~]$ sudo mkdir /data
```

6. Use o comando a seguir para montar o volume no diretório que você criou na etapa anterior.

```
[ec2-user ~]$ sudo mount /dev/xvdf /data
```

7. Revise as permissões de arquivo da montagem do seu novo volume para assegurar-se de que os usuários e aplicações podem gravar no volume. Para mais informações sobre as permissões de arquivos, consulte [Segurança de arquivos](#) no Projeto de documentação do Linux.
8. O ponto de montagem não é preservado automaticamente após a reinicialização da instância. Para montar automaticamente esse volume do EBS após a reinicialização, consulte [Montar automaticamente um volume anexado após a reinicialização \(p. 1285\)](#).

## Montar automaticamente um volume anexado após a reinicialização

Para montar um volume anexado do EBS em cada reinicialização do sistema, adicione uma entrada para o dispositivo ao arquivo `/etc/fstab`.

Você pode usar o nome do dispositivo, como `/dev/xvdf`, no `/etc/fstab`, mas recomendamos o uso do identificador universal exclusivo (UUID) de 128 bits do dispositivo. Os nomes dos dispositivos podem mudar, mas o UUID persiste durante todo o ciclo de vida da partição. Usando o UUID, você reduz as possibilidades de o sistema se tornar não inicializável após uma reconfiguração de hardware. Para obter mais informações, consulte [Identificar o dispositivo EBS \(p. 1435\)](#).

Para montar um volume anexado automaticamente após a reinicialização

1. (Opcional) Crie um backup do seu arquivo `/etc/fstab` para usar se você destruir ou excluir acidentalmente esse arquivo quando for editá-lo.

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

2. Use o comando blkid para encontrar o UUID do dispositivo. Anote o UUID do dispositivo que você deseja montar após a reinicialização. Você vai precisar dele na etapa seguinte.

Por exemplo, o comando a seguir mostra que existem dois dispositivos montados na instância e mostra os UUIDs para ambos os dispositivos.

```
[ec2-user ~]$ sudo blkid  
/dev/xvda1: UUID="/" UUID="ca774df7-756d-4261-a3f1-76038323e572" TYPE="xfs"  
PARTLABEL="Linux" PARTUUID="02dc367-e87c-4f2e-9a72-a3cf8f299c10"  
/dev/xvdf: UUID="aebf131c-6957-451e-8d34-ec978d9581ae" TYPE="xfs"
```

Para Ubuntu 18.04, use o comando lsblk.

```
[ec2-user ~]$ sudo lsblk -o +UUID
```

3. Abra o arquivo /etc/fstab usando qualquer editor de texto (como nano ou vim).

```
[ec2-user ~]$ sudo vim /etc/fstab
```

4. Adicione a entrada a seguir ao /etc/fstab para montar o dispositivo no ponto de montagem especificado. Os campos são o valor de UUID retornado pelo blkid (ou lsblk, para Ubuntu 18.04), ponto de montagem, sistema de arquivos e opções recomendadas de montagem do sistema de arquivos. Para obter mais informações sobre os campos obrigatórios, execute man fstab para abrir o fstab manual.

No exemplo a seguir, montamos o dispositivo com UUID aebf131c-6957-451e-8d34-ec978d9581ae no ponto de montagem /data e usamos o sistema de arquivos xfs. Também usamos as flags defaults e nofail. Especificamos 0 para evitar que o sistema de arquivos seja despejado, e especificamos 2 para indicar que ele é um dispositivo não raiz.

```
UUID=aebf131c-6957-451e-8d34-ec978d9581ae /data xfs defaults,nofail 0 2
```

#### Note

Se você inicializar a instância sem esse volume anexado (por exemplo, depois de mover o volume para outra instância), a opção de montagem nofail permitirá que a instância seja inicializada mesmo se houver erros na montagem do volume. Os derivados de Debian, incluindo versões de Ubuntu anteriores à 16.04, também devem adicionar a opção de montagem nobootwait.

5. Para verificar se sua entrada funciona, execute os seguintes comandos para desmontar o dispositivo e, depois, montar todos os sistemas de arquivos em /etc/fstab. Se não houver erros, o arquivo /etc/fstab será válido e o sistema de arquivos será montado automaticamente após ser reinicializado.

```
[ec2-user ~]$ sudo umount /data  
[ec2-user ~]$ sudo mount -a
```

Se você receber uma mensagem de erro, resolva os erros no arquivo.

#### Warning

Erros no arquivo /etc/fstab podem impedir a inicialização de um sistema. Não desative um sistema que tenha erros no arquivo /etc/fstab.

Se você não souber corrigir os erros no /etc/fstab e criou um arquivo de backup na primeira etapa desse procedimento, poderá restaurar a partir do arquivo de backup usando o comando a seguir.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

## 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 \(p. 1551\)](#).

### 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 \(p. 1477\)](#).

## 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 Linux da instância. Por exemplo, use o comando a seguir:

```
[ec2-user ~]$ df -hT /dev/xvda1
Filesystem      Type      Size  Used Avail Use% Mounted on
/dev/xvda1        xfs      8.0G  1.2G  6.9G  15%  /
```

Para obter informações sobre como visualizar o espaço livre em disco em uma instância do Windows, consulte [View free disk space \(Ver espaço livre em disco\)](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## 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 \(p. 1303\)](#).

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 \(p. 1289\)](#)
- [Substituir um volume de dados \(p. 1292\)](#)

## 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 \(p. 1290\)](#).

#### Tópicos

- [Considerations \(p. 337\)](#)
- [Substituir um volume raiz \(p. 1290\)](#)
- [Exibir tarefas de substituição do volume raiz \(p. 1290\)](#)

## 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 \(p. 1275\)](#).
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 Linux \(p. 1283\)](#).

## 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 \(p. 1292\)](#)
- [Eventos de volume do EBS \(p. 1295\)](#)
- [Trabalhar com um volume danificado \(p. 1296\)](#)
- [Trabalhar com o atributo de volume de E/S habilitada automaticamente \(p. 1298\)](#)

Para obter informações adicionais sobre o monitoramento, consulte [Métricas do Amazon CloudWatch para o Amazon EBS \(p. 1477\)](#) e [Amazon CloudWatch Events para Amazon EBS \(p. 1484\)](#).

### 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 `fsck`, 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 \(p. 1288\)](#).

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 \(p. 1466\)](#).

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)

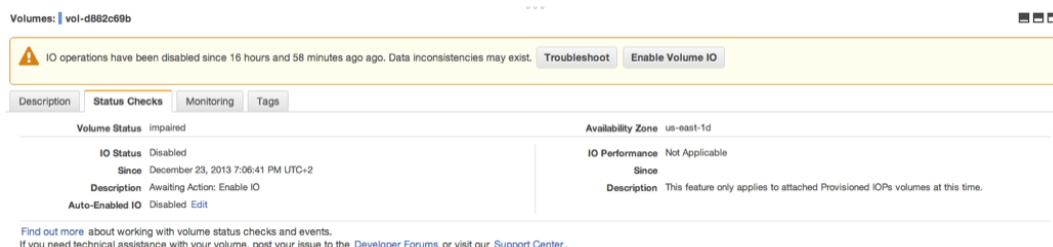
Status dos volumes	Status de E/S habilitado	Status d performance de E/S (somente volumes <b>io1</b> e <b>io2</b> )
<b>warning</b>	Habilitado (E/S habilitada ou E/S habilitada automaticamente)	Degradoado (a performance do volume está abaixo das expectativas)  Seramente degradado (a performance do volume está muito abaixo das expectativas)
<b>impaired</b>	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)
<b>insufficient-data</b>	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 \(p. 1296\)](#).

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 \(p. 1295\)](#).

#### 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) (`autoEnableIOOnA API`). Para obter mais informações sobre como alterar esse atributo, consulte [Trabalhar com um volume danificado \(p. 1296\)](#).

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.

The screenshot shows the AWS CloudWatch Events console with the following details:

Resource Name	Resource Type	Resource Id	Availability Zone	Event Type	Event Description	Event Status	Start Time	Duration	Event Progress
vol-0381c540	volume	vol-0381c540	us-east-1d	potential-data-i...	Awaiting Action...	⚠ Awaiting A...	December 23, ...	30 days, 15 ho...	IO Disabled
vol-3682c675	volume	vol-3682c675	us-east-1d	potential-data-i...	Awaiting Action...	⚠ Awaiting A...	December 23, ...	30 days, 15 ho...	IO Disabled

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](#).*

**Enable Volume IO**

## 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 \(p. 1296\)](#). 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 \(p. 1296\)](#)
- [Opção 2: executar uma verificação de consistência no volume usando outra instância \(p. 1297\)](#)
- [Opção 3: excluir o volume se não precisar mais dele \(p. 1298\)](#)

### Opção 1: executar uma verificação de consistência no volume anexado a sua instância

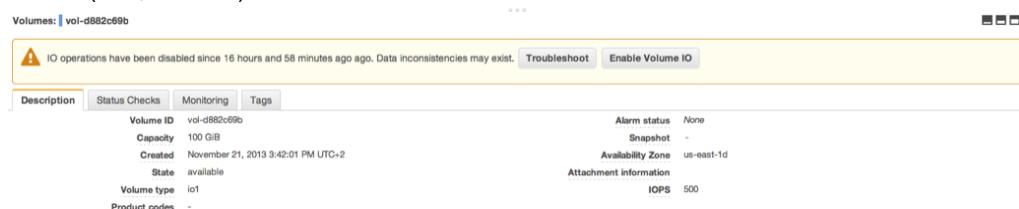
A opção mais simples é habilitar a E/S e executar uma verificação de consistência dos dados no volume enquanto o volume ainda estiver anexado a sua instância do Amazon EC2.

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 fsck.
  - 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.

#### Opção 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

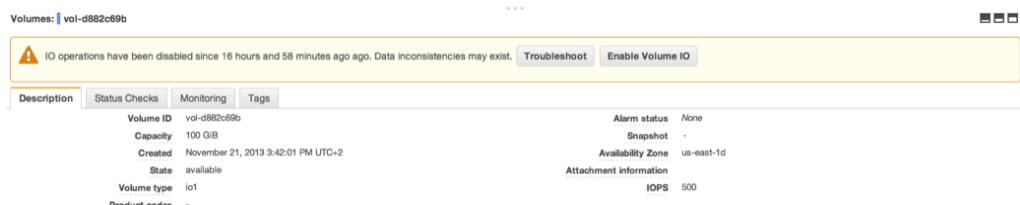
Este procedimento pode causar a perda de E/Ss de gravação que foram suspensas quando a E/S do volume foi desabilitada.

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 Linux \(p. 1300\)](#).
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 \(p. 509\)](#) e [Vincular um volume de Amazon EBS a uma instância \(p. 1277\)](#).
  5. Verifique os dados no volume.
    - a. Execute o comando `fsck`.
    - 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 \(p. 1302\)](#).

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 \(p. 1275\)](#).

## 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

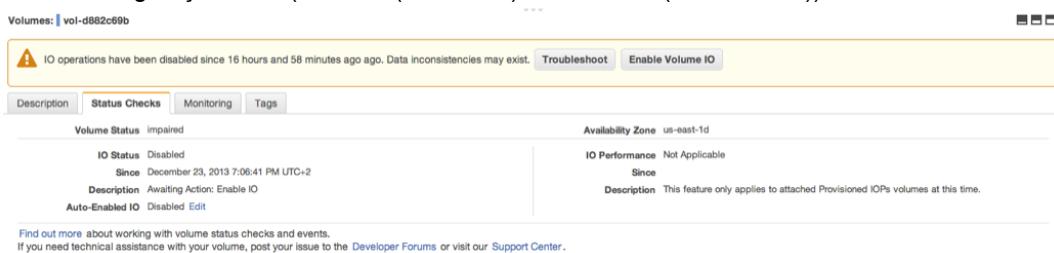
que você saiba que o volume estava em um estado de potencialmente inconsistente, mas que sua E/S foi habilitada automaticamente. Quando esse evento ocorre, você deve verificar a consistência do volume e substitui-lo se necessário. Para obter mais informações, consulte [Eventos de volume do EBS \(p. 1295\)](#).

Você pode exibir e modificar o atributo Auto-Enabled IO (E/S habilitado automaticamente) de um volume usando os seguintes métodos.

#### Console

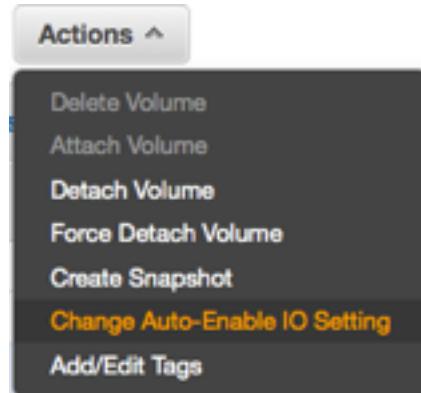
Para visualizar o atributo de E/S habilitado automaticamente de um volume

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.

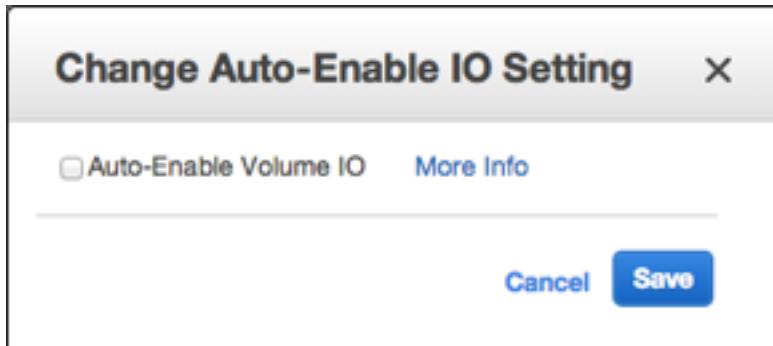


Para modificar o atributo de E/S habilitado automaticamente de um volume

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 Linux

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 desanexar volumes de uma instância do Windows, consulte [Desanexar um volume de uma instância do Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

#### Tópicos

- [Considerations \(p. 337\)](#)
- [Desmontar e desanexar um volume \(p. 1301\)](#)
- [Troubleshoot \(p. 1301\)](#)

## 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 \(p. 1302\)](#).

## 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. \(p. 1301\)](#)
- [Etapa 2: desanexar o volume da instância. \(p. 1301\)](#)

#### Etapa 1: desmonte o volume.

Na instância do Linux, use o comando a seguir para desmontar o dispositivo `/dev/sdh`.

```
[ec2-user ~]$ umount -d /dev/sdh
```

#### 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 \(AWS Tools for Windows PowerShell\)](#)

## 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 Linux \(p. 1300\)](#).

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 \(p. 1307\)](#).

Ao excluir um snapshot, somente os dados exclusivos desse snapshot serão removidos. Para obter mais informações, consulte [Excluir um snapshot do Amazon EBS \(p. 1310\)](#).

#### 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 \(p. 1487\)](#).

#### 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 \(p. 1307\)](#).

#### 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 \(p. 1304\)](#)
- [Copiar e compartilhar snapshots \(p. 1306\)](#)
- [Suporte a criptografia para snapshots \(p. 1307\)](#)
- [Criar snapshots de Amazon EBS \(p. 1307\)](#)
- [Excluir um snapshot do Amazon EBS \(p. 1310\)](#)
- [Copiar um snapshot do Amazon EBS. \(p. 1313\)](#)
- [Exibir informações do snapshot do Amazon EBS \(p. 1318\)](#)
- [Compartilhar um snapshot do Amazon EBS \(p. 1319\)](#)
- [Amazon EBS local snapshots on Outposts \(p. 1323\)](#)
- [Usar o APIs diretas do EBS para acessar o conteúdo de um snapshot do EBS \(p. 1333\)](#)
- [Automatizar o ciclo de vida do snapshot \(p. 1359\)](#)

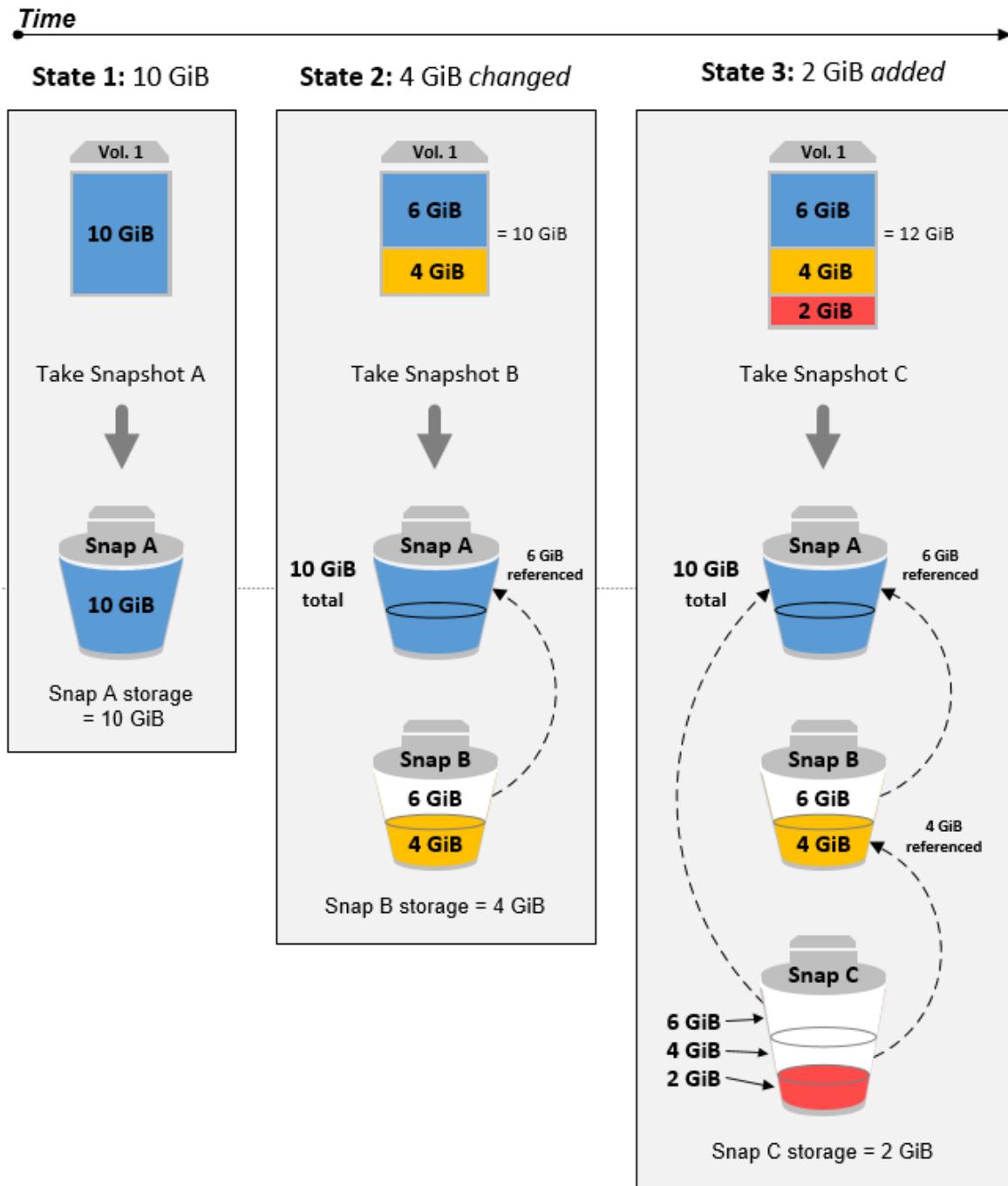
## Como funcionam os snapshots incrementais

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

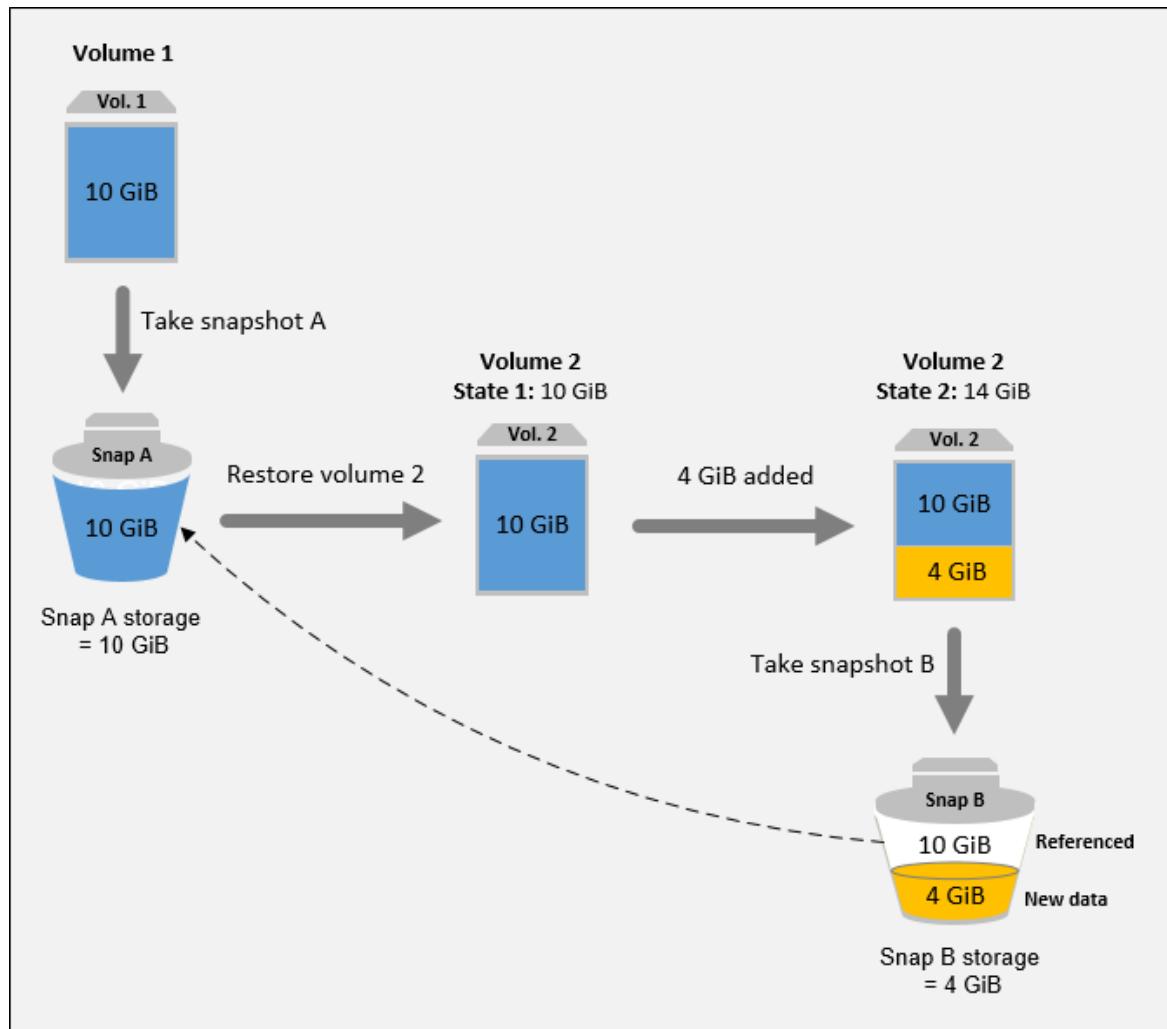
O diagrama nesta seção mostra como snapshots incrementais podem ser obtidos de diferentes volumes.

#### 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 \(p. 1310\)](#).

## 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 \(p. 1319\)](#).

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 \(p. 1275\)](#). 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 \(p. 1313\)](#).

## Supporte 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 \(p. 1307\)](#) e em [Copiar um snapshot do Amazon EBS \(p. 1313\)](#).

Para obter mais informações, consulte [Criptografia de Amazon EBS \(p. 1418\)](#).

## Criar snapshots de Amazon EBS

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 \(p. 1552\)](#).

## 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 \(p. 1418\)](#).

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 \(p. 1319\)](#).

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 \(p. 1319\)](#).

## 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 \(p. 1359\)](#).

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 \(`createSnapshots`\) \(p. 1488\)](#).

## 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 \(p. 1359\)](#).

## 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)

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 \(createSnapshots\) \(p. 1488\)](#).

## 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. \(p. 1313\)](#)
- [Compartilhar um snapshot do Amazon EBS \(p. 1319\)](#)
- [Criar um volume a partir de um snapshot \(p. 1275\)](#)

## 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.

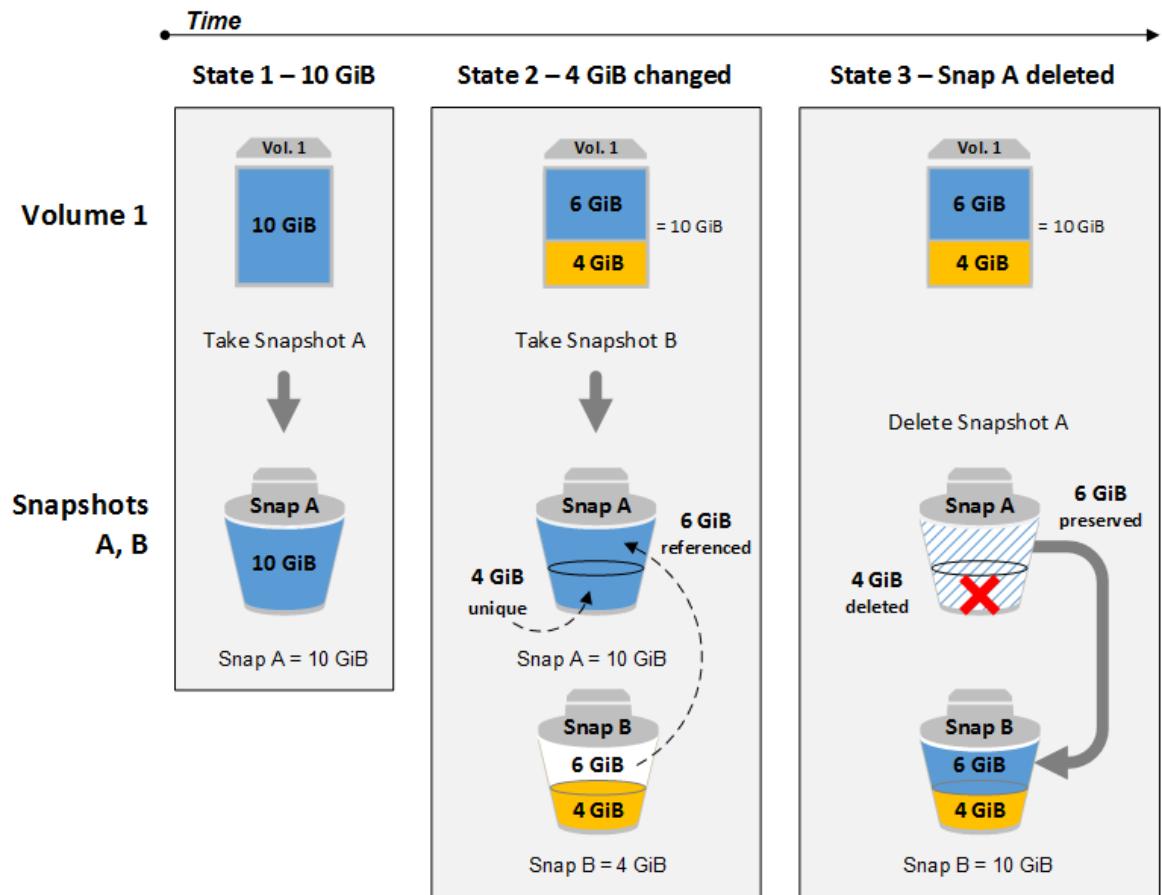
Ao excluir um snapshot, somente os dados mencionados exclusivamente por esse snapshot são removidos. Os dados exclusivos só serão excluídos se todos os snapshots que fazem referência a eles forem excluídos. A exclusão de snapshots anteriores de um volume não afeta sua capacidade de criar volumes de snapshots 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 \(p. 1304\)](#) 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 AMI do Linux \(p. 159\)](#).
- 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 \(p. 1359\)](#).
- 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 \(p. 1319\)](#).

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 \(p. 1552\)](#).
- 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 \(p. 1489\)](#) 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 \(p. 1319\)](#).

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 \(p. 1421\)](#) (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 \(p. 1315\)](#)
- [Resultados de criptografia: copiar snapshots compartilhados com você \(p. 1316\)](#)

### [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 <b>Encrypted</b> 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 <b>Encrypted</b> 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 <b>Encrypted</b> 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. 1421), 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 \(p. 1319\)](#)
- [Compartilhar um snapshot \(p. 1320\)](#)
- [Compartilhar uma chave do KMS \(p. 1321\)](#)
- [Exibir snapshots que são compartilhados com você \(p. 1322\)](#)
- [Usar snapshots que são compartilhados com você \(p. 1323\)](#)
- [Determinar o uso de snapshots compartilhados por você \(p. 1323\)](#)

## 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. \(p. 1313\)](#).

- 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. 1321).

## 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 \(p. 1322\)](#). 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 \(p. 1322\)](#). 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 \(p. 919\)](#).

## 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 \(p. 1303\)](#).

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 \(p. 1324\)](#)
- [Prerequisites \(p. 1325\)](#)
- [Considerations \(p. 337\)](#)
- [Controlar o acesso com o IAM \(p. 1326\)](#)
- [Trabalhe com snapshots locais \(p. 1327\)](#)

## 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 \(p. 1303\)](#).

### 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 \(p. 1326\)](#).

### 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 \(p. 1327\)](#). 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 \(p. 1333\)](#).

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 \(p. 1332\)](#).

- 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 \(p. 1331\)](#).
- 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 \(p. 1326\)](#).
- 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 \(p. 1304\)](#).
- 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 \(p. 1326\)](#)
- [Impeça que as entidades excluam snapshots locais \(p. 1327\)](#)

### 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 \(p. 1328\)](#)
- [Crie snapshots locais a partir de volumes em um Outpost \(p. 1328\)](#)
- [Crie snapshots locais multivolume a partir de instâncias em um Outpost \(p. 1329\)](#)
- [Crie AMIs em snapshots locais \(p. 1330\)](#)
- [Copiar snapshots de uma região da AWS para um Outpost \(p. 1331\)](#)
- [Copiar AMIs de uma região da AWS para um Outpost \(p. 1332\)](#)

- [Crie volumes a partir de snapshots locais \(p. 1332\)](#)
- [Execute instâncias a partir de AMIs baseadas em snapshots locais \(p. 201\)](#)
- [Exclua snapshots locais \(p. 1332\)](#)
- [Automatize snapshots em um Outpost \(p. 1333\)](#)

## 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 \(p. 1331\)](#).
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 \(p. 1329\)](#).
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 \(p. 1328\)](#) ou [Crie snapshots locais multivolume a partir de instâncias em um Outpost \(p. 1329\)](#).

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 \(p. 1275\)](#).

## 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 \(p. 1312\)](#).

## 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 \(p. 1364\)](#) (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 \(p. 1334\)](#)
- [Permissões para usuários do IAM \(p. 1337\)](#)
- [Usar criptografia \(p. 1341\)](#)
- [Usar a assinatura do Signature versão 4. \(p. 1341\)](#)
- [Usar somas de verificação \(p. 1342\)](#)
- [Trabalhar com as APIs diretas do EBS usando a API ou AWS SDKs \(p. 1342\)](#)
- [Como trabalhar com as APIs diretas do EBS usando a linha de comando \(p. 1347\)](#)
- [Otimizar a performance \(p. 1350\)](#)
- [Perguntas frequentes \(p. 1350\)](#)
- [Registrar chamadas de API para as APIs diretas do EBS com o AWS CloudTrail \(p. 1351\)](#)
- [APIs diretas do EBS e VPC endpoints de interface \(p. 1357\)](#)
- [Idempotência para a API StartSnapshot \(p. 1358\)](#)

## 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 \(p. 1303\)](#).

#### 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 \(p. 1342\)](#) 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 \(p. 1341\)](#) 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 \(p. 1342\)](#) e [Como trabalhar com as APIs diretas do EBS usando a linha de comando \(p. 1347\)](#) mais adiante neste guia.

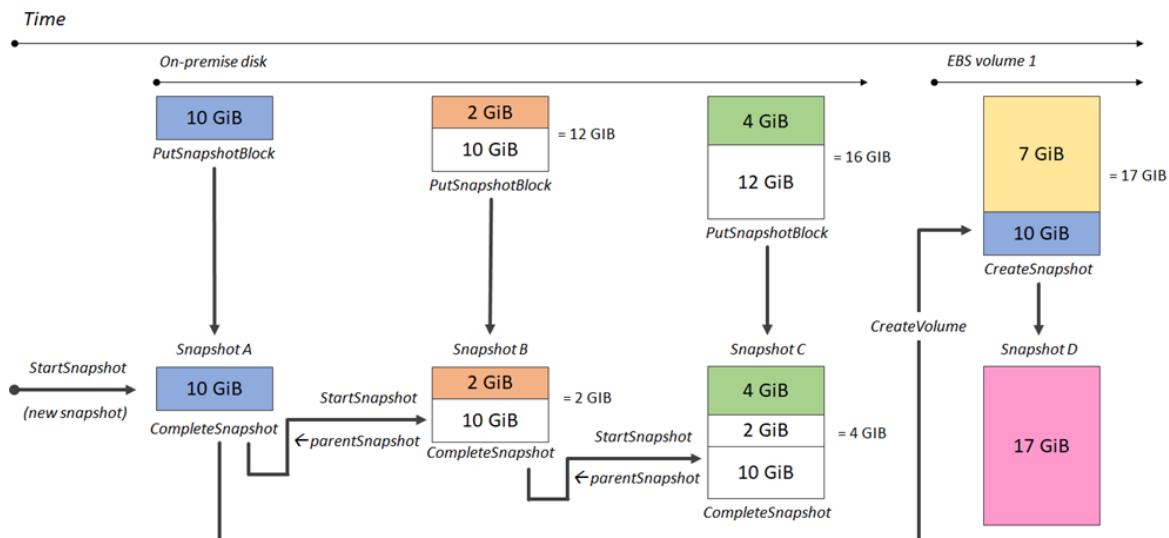
### [Usar as APIs diretas do EBS para gravar snapshots incrementais](#)

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 \(p. 1342\)](#) e [Como trabalhar com as APIs diretas do EBS usando a linha de comando \(p. 1347\)](#) 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": "  
                <ARN>  
            "  
        }  
    ]  
}
```

```
        "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. \(p. 1313\)](#) e [Criptografia por padrão \(p. 1421\)](#).

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 \(p. 1421\)](#).

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 \(p. 1337\)](#) 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. \(p. 1341\)](#).

### 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": "AAUBAWudwfmofcrQhGV1LwuRKm2b8ZXPiyrqoykTRC6IU1NbxEWDY1pPjvnV"
        },
        {
            "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-DataLength: 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 \(p. 1358\)](#).

```
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/3jJzI2crq2eFDCgHmyNf777e1D9oVR"
        },
        {
            "BlockIndex": 6001,
            "FirstBlockToken": "AAABASBpSJ2UAD3PLxJnCt6zun4/T4sU25Bnb8jb5Q6FRXHFqAIAqE04hJoR"
        },
        {
            "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/T4sU25Bnb8jb5Q6FRXHFqAIAqE04hJoR`, 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/T4sU25Bnb8jb5Q6FRXHFqAIAqE04hJoR 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 \(p. 1358\)](#).

```
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 \(p. 1342\)](#) 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 \(p. 1350\)](#).

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 \(p. 1337\)](#) 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 \(p. 1351\)](#).

## [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,
```

```
        "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`.

```
$ 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 \(p. 1359\)](#).

## 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 \(p. 1359\)](#)
- [Considerações para o Amazon Data Lifecycle Manager \(p. 1362\)](#)
- [Automação dos ciclos de vida do snapshot \(p. 1364\)](#)
- [Automatizar ciclos de vida da AMI \(p. 1372\)](#)
- [Automatizar cópias de snapshots entre contas \(p. 1378\)](#)
- [Exibir, modificar e excluir políticas de ciclo de vida \(p. 1387\)](#)
- [AWS Identity and Access Management \(p. 1390\)](#)
- [Monitorar o ciclo de vida de snapshots e AMIs \(p. 1396\)](#)

## Como Amazon Data Lifecycle Manager funciona

Veja a seguir os elementos de chaves do Amazon Data Lifecycle Manager.

### Elementos

- [Snapshots \(p. 1360\)](#)
- [AMIs apoiadas pelo EBS \(p. 1360\)](#)
- [Tags de recurso de destino \(p. 1360\)](#)
- [Tags do Amazon Data Lifecycle Manager \(p. 1360\)](#)

- [Políticas de ciclo de vida \(p. 1360\)](#)
- [Programações de política \(p. 1361\)](#)

## 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 \(p. 1303\)](#).

## 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 \(AMIs\) \(p. 72\)](#).

## 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 \(p. 1552\)](#).

## 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 \(p. 1308\)](#). 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 \(p. 1361\)](#).
- Retenção—Especifica como os snapshots ou AMIs devem ser reterados. 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 \(p. 1430\)](#):

- 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 \(p. 1434\)](#).

#### 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 às políticas de ciclo de vida de snapshot e aos volumes habilitados para [multi-attach \(p. 1278\)](#):

- Ao criar uma política de ciclo de vida com base em tags de instâncias para snapshots de vários volumes, o Amazon Data Lifecycle Manager inicia um snapshot do volume para cada instância anexada. Use a tag timestamp para identificar o conjunto de snapshots consistentes em relação ao tempo criados das instâncias anexadas.

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.

Se você não habilitar o cancelamento automático de compartilhamento, o snapshot será compartilhado até ser excluído.

- 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 necessárias, 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, escolha AWS 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.

- 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.
- Selezione 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::123456789010: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 reinicializa 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",  
        "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 \  
--rule-name MyAMIrule
```

```
--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 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 \(p. 1379\)](#)
- [Especificar filtros de descrição de snapshot \(p. 1386\)](#)

## 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 \(conta de origem\) \(p. 1379\)](#)
- [Etapa 2: Compartilhe a chave gerenciada pelo cliente \(Conta de origem\) \(p. 1379\)](#)
- [Etapa 3: criar política de eventos de cópia entre contas \(conta de destino\) \(p. 1381\)](#)
- [Etapa 4: permitir que a função do IAM use as Chaves do KMS necessárias \(conta de destino\) \(p. 1384\)](#)

### 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 \(Conta de origem\) \(p. 1379\)](#).

Para obter mais informações sobre como criar um snapshot de política do EBS, consulte [Automação dos ciclos de vida do snapshot \(p. 1364\)](#).

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 das 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:PutGrant"
    ]
}
```

```
        "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 \(p. 1386\)](#).
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. 1384).

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 [Especificando filtros de descrição de snapshot](#) (p. 1386).
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 \(conta de destino\) \(p. 1384\)](#).

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 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.
  - 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,
            "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 descritivo 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: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 \(p. 1387\)](#)
- [Modificar políticas de ciclo de vida \(p. 1388\)](#)
- [Excluir políticas de ciclo de vida \(p. 1282\)](#)

## 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": "snapshot"
                        }
                    ]
                }
            ]
        }
    }
}
```

```
        "Key": "type"
    }
],
"RetainRule": {
    "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.

```
        "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. 1390)
  - Funções de serviço da IAM (p. 1393)
  - Permissões para usuários do IAM (p. 1395)
  - Permissões para criptografia (p. 1396)

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 \(p. 1645\)](#).

Alteração	Descrição	Data
AWSDataLifecycleManager adicionou as ações ec2:EnableImageDeprecation e ec2:DisableImageDeprecation para conceder permissão de políticas de AMI apoiadas pelo EBS para habilitar e desabilitar a defasagem da AMI.	O Amazon Data Lifecycle Manager adicionou as ações ec2:EnableImageDeprecation e ec2:DisableImageDeprecation para conceder permissão de políticas de AMI apoiadas pelo EBS para habilitar e desabilitar a defasagem da AMI.	23 de agosto de 2021
O Amazon Data Lifecycle Manager começou a monitorar	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 \(p. 1393\)](#)
- [Funções de serviço personalizadas para o Amazon Data Lifecycle Manager \(p. 1394\)](#)

## 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 \(p. 1396\)](#)
- [AWS CloudTrail \(p. 1397\)](#)
- [Monitorar políticas usando o CloudWatch Events \(p. 1397\)](#)
- [Monitorar políticas usando o Amazon CloudWatch \(p. 1398\)](#)

### 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 \(p. 1387\)](#).

## 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 \(p. 1484\)](#).
- `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 \(p. 1398\)](#)
- [Visualizar métricas do CloudWatch para suas políticas \(p. 1401\)](#)
- [Métricas de gráfico para suas políticas \(p. 1402\)](#)
- [Criar um alarme do CloudWatch para uma política \(p. 1403\)](#)
- [Exemplo de casos de uso do \(p. 150\)](#)
- [Gerenciamento de políticas que relatam ações com falha \(p. 1405\)](#)

### 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.
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.
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.
ImagesCopiedRegionDeleted	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](#).

```
$ 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`.

```
$ 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`.

```
$ 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 de cópia de snapshots entre contas concluída (com base em `SnapshotsCopiedAccountDeleteCompleted`)
- Falha na exclusão de 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 \(p. 1403\)](#)
- [Exemplo 2: métrica SnapshotDeleteFailed \(p. 1404\)](#)
- [Exemplo 3: métrica SnapshotsCopiedRegionFailed \(p. 1404\)](#)

### 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:

```
$ 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 `SnapshotDeleteFailed` 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:

```
$ 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:

```
$ 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 \(p. 1405\)](#)
- [Criptografia de Amazon EBS \(p. 1418\)](#)
- [Restauração rápida de snapshots do Amazon EBS \(p. 1430\)](#)

## 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 \(p. 1405\)](#)
- [Solicitar modificações para seus volumes do EBS \(p. 1407\)](#)
- [Monitorar o progresso das modificações de volume \(p. 1411\)](#)
- [Estender um sistema de arquivos Linux após um redimensionamento de volume \(p. 1414\)](#)

## 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 \(p. 1271\)](#).

### Tópicos

- [Tipos de instâncias compatíveis \(p. 1405\)](#)
- [Requisitos para volumes do Linux \(p. 1406\)](#)
- [Limitations \(p. 1406\)](#)

## Tipos de instâncias compatíveis

Elastic Volumes são compatíveis com as seguintes instâncias:

- [Todas as instâncias da geração atual \(p. 204\)](#)

- 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 \(p. 1410\)](#).

### Requisitos para volumes do Linux

As AMIs do Linux exigem uma tabela de partição GUID (GPT) e GRUB 2 para volumes de inicialização de 2 TiB (2048 GiB) ou maiores. Muitas AMIs do Linux atualmente ainda usam o esquema de particionamento de MBR, que só é compatível com tamanhos de volume de inicialização de 2 TiB. Se sua instância não for inicializada com um volume de inicialização superior a 2 TiB, a AMI que você está usando pode ser limitada a um tamanho de volume de inicialização inferior a 2 TiB. Volumes de não inicialização não têm essas limitações nas instâncias do Linux. Para requisitos que afetam os volumes do Windows, consulte [Requisitos para volumes do Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Antes de tentar redimensionar um volume de inicialização além de 2 TiB, você pode determinar se o volume está usando particionamento MBR ou GPT ao executar o seguinte comando na sua instância:

```
[ec2-user ~]$ sudo gdisk -l /dev/xvda
```

Uma instância Amazon Linux com particionamento GPT retorna as seguintes informações:

```
GPT fdisk (gdisk) version 0.8.10

Partition table scan:
  MBR: protective
  BSD: not present
  APM: not present
  GPT: present

Found valid GPT with protective MBR; using GPT.
```

Uma instância SUSE com particionamento MBR retorna as seguintes informações:

```
GPT fdisk (gdisk) version 0.8.8

Partition table scan:
  MBR: MBR only
  BSD: not present
  APM: not present
  GPT: not present
```

### 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 \(p. 1409\)](#).
- 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 de Amazon EBS \(p. 1466\)](#).
- 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 \(p. 1271\)](#).
- 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 \(p. 1253\)](#)
- 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 rsync.
- 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 \(p. 1262\)](#)
- 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 \(p. 1307\)](#).
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 \(p. 1411\)](#).
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 Linux após um redimensionamento de volume \(p. 1414\)](#).

## Tópicos

- [Modificar um volume do EBS usando volumes elásticos \(p. 1408\)](#)
- [Inicializar o suporte aos Elastic Volumes \(se necessário\) \(p. 1409\)](#)
- [Modificar um volume do EBS se não houver suporte para Elastic Volumes \(p. 1410\)](#)

## 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 Linux após um redimensionamento de volume \(p. 1414\)](#) .

### 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,  
        "VolumeId": "vol-1111111111111111",  
        "VolumeType": "io1",  
        "Iops": 10000  
    }  
}
```

```
        "TargetVolumeType": "io1",
        "ModificationState": "modifying",
        "VolumeId": "vol-1111111111111111",
        "TargetIops": 10000,
        "StartTime": "2017-01-19T22:21:02.959Z",
        "Progress": 0,
        "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 Linux após um redimensionamento de volume \(p. 1414\)](#).

### Inicializar 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-e6b46410: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. Em Linux, use o comando `df -h` para verificar o tamanho do sistema de arquivos.

```
[ec2-user ~]$ df -h  
Filesystem      Size  Used Avail Use% Mounted on  
/dev/xvda1       7.9G  943M  6.9G  12% /  
tmpfs           1.9G     0  1.9G   0% /dev/shm
```

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 Linux após um redimensionamento de volume \(p. 1414\)](#).

## 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).

**Amazon Elastic Compute Cloud Manual**  
**do usuário para instâncias do Linux**  
**Serviços de dados do EBS**

The screenshot shows the AWS Management Console interface for EBS volumes. At the top, there's a table listing several volumes with columns for Name, Volume ID, Size, Volume Type, IOPS, Snapshot, Created, Availability Zone, and State. One volume, 'vol-02940f6ee433f...', is selected and highlighted with a blue border. Below the table, a modal window titled 'Volume modification details' provides specific information about the selected volume's modification. It includes fields for Original Volume Type (gp2), Original Size (8), Original IOPS (100), Target Volume Type (gp2), Target Size (16), and Target IOPS (100). The 'Status message' field is empty. To the right of the modal, there are additional volume details such as 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 Linux após um redimensionamento de volume

Depois de [aumentar o tamanho de um volume do EBS \(p. 1407\)](#), é necessário usar comandos específicos do sistema de arquivos para estender o sistema de arquivos ao tamanho maior. Você pode redimensionar o sistema de arquivos à medida que o volume entrar no estado `optimizing`.

### Important

Antes de estender um sistema de arquivos que contém dados valiosos, a prática recomendada é criar um snapshot do volume, caso você precise reverter suas alterações. Para obter mais informações, consulte [Criar snapshots de Amazon EBS \(p. 1307\)](#). Se sua AMI do Linux usa o esquema de particionamento do MBR, você está limitado a um volume de inicialização de até 2 TiB. Para obter mais informações, consulte [Requisitos para volumes do Linux \(p. 1406\)](#) e [Restrições de tamanho e configuração de um volume do EBS \(p. 1271\)](#).

O processo para estender um sistema de arquivos no Linux é o seguinte:

1. O volume do EBS pode ter uma partição com o sistema de arquivos e os dados. Aumentar o tamanho de um volume não aumenta o tamanho da partição. Antes de estender o sistema de arquivos em um volume redimensionado, verifique se o volume tem uma partição que deve ser estendida para o novo tamanho do volume.
2. Use o comando específico do sistema de arquivos para redimensionar cada sistema de arquivos de acordo com a capacidade do novo volume.

Para obter informações sobre como estender um sistema de arquivos do Windows, consulte [Estender um sistema de arquivos do Windows após redimensionar um volume](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Os exemplos a seguir demonstram o processo de extensão de um sistema de arquivos Linux. Para sistemas de arquivos e esquemas de particionamento diferentes dos mostrados aqui, consulte a documentação desses sistemas de arquivos e esquemas de particionamento para obter instruções.

### Note

Se você estiver usando volumes lógicos no volume do Amazon EBS, você deve usar o Logical Volume Manager (LVM) para estender o volume lógico. Para obter instruções sobre como fazer isso, consulte a seção Extend the logical volume (Estender o volume lógico) no artigo [How do I create an LVM logical volume on an entire EBS volume? \(Como criar um volume lógico LVM em todo um volume do EBS?\)](#) da Central de Conhecimento da AWS .

### Exemplos

- [Para estender o sistema de arquivos de volumes EBS de NVMe \(p. 1415\)](#)
- [Exemplo: estender o sistema de arquivos de volumes do EBS \(p. 1416\)](#)

## Para estender o sistema de arquivos de volumes EBS de NVMe

Para este exemplo, suponha que você tenha uma instância criada no [Sistema Nitro \(p. 210\)](#), como uma instância M5. Você redimensionou o volume de inicialização de 8 GB para 16 GB e um volume adicional de 8 GB para 30 GB. Use o procedimento a seguir para estender o sistema de arquivos dos volumes redimensionados.

### Para estender o sistema de arquivos de volumes EBS de NVMe

1. [Conecte-se à sua instância \(p. 535\)](#).
2. Para verificar o sistema de arquivos para cada volume, use o comando df -hT.

```
[ec2-user ~]$ df -hT
```

O exemplo a seguir mostra uma saída de exemplo de uma instância que tem um volume de inicialização com um sistema de arquivos XFS e um volume adicional com um sistema de arquivos XFS. A convenção de nomenclatura /dev/nvme[0-26]n1 indica que os volumes são expostos como dispositivos de blocos NVMe.

```
[ec2-user ~]$ df -hT
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/nvme0n1p1  xfs   8.0G  1.6G  6.5G  20% /
/dev/nvme1n1    xfs   8.0G   33M  8.0G   1% /data
...
...
```

3. Para verificar se o volume tem uma partição que deve ser estendida, use o comando lsblk para exibir informações sobre os dispositivos de blocos NVMe conectados à instância.

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1   259:0    0  30G  0 disk /data
nvme0n1   259:1    0  16G  0 disk
##nvme0n1p1 259:2    0   8G  0 part /
##nvme0n1p128 259:3   0   1M  0 part
```

Este exemplo de saída mostra o seguinte:

- O volume raiz, /dev/nvme0n1, tem uma partição, /dev/nvme0n1p1. Enquanto o tamanho do volume raiz reflete o novo tamanho, 16 GB, o tamanho da partição reflete o tamanho original, 8 GB, e deve ser estendido antes que você possa estender o sistema de arquivos.
  - O volume /dev/nvme1n1 não tem partições. O tamanho do volume reflete o novo tamanho, 30 GB.
4. Para volumes que têm uma partição, como o volume raiz mostrado na etapa anterior, use o comando growpart para estender a partição. Observe que há um espaço entre o nome do dispositivo e o número da partição.

```
[ec2-user ~]$ sudo growpart /dev/nvme0n1 1
```

5. (Opcional) Use o comando lsblk novamente para verificar se a partição reflete o tamanho do volume aumentado.

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
nvme1n1   259:0    0  30G  0 disk /data
nvme0n1   259:1    0  16G  0 disk
##nvme0n1p1 259:2    0  16G  0 part /
##nvme0n1p128 259:3   0   1M  0 part
```

6. Use o comando df -h para verificar o tamanho do sistema de arquivos de cada volume. Neste exemplo de saída, ambos os sistemas de arquivos refletem o tamanho original do volume, 8 GB.

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/nvme0n1p1   8.0G  1.6G  6.5G  20% /
/dev/nvme1n1     8.0G   33M  8.0G   1% /data
...
```

7. Para estender o sistema de arquivos em cada volume, use o comando correto para seu sistema de arquivos, como segue:

- [Sistema de arquivos XFS] Use o comando xfs\_growfs para estender o sistema de arquivos em cada volume. Neste exemplo, / e /data são os pontos de montagem de volume mostrados na saída de df -h.

```
[ec2-user ~]$ sudo xfs_growfs -d /
[ec2-user ~]$ sudo xfs_growfs -d /data
```

Se as ferramentas do XFS ainda não estiverem instaladas, você poderá instalá-las da seguinte forma.

```
[ec2-user ~]$ sudo yum install xfsprogs
```

- [Sistema de arquivos ext4] Use o comando resize2fs para estender o sistema de arquivos em cada volume.

```
[ec2-user ~]$ sudo resize2fs /dev/nvme0n1p1
[ec2-user ~]$ sudo resize2fs /dev/nvme1n1
```

- [Outro sistema de arquivos] Para estender o sistema de arquivos em cada volume, consulte a documentação do sistema de arquivos para obter instruções.

8. (Opcional) Use o comando df -h novamente para verificar se cada sistema de arquivos reflete o tamanho do volume aumentado.

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/nvme0n1p1   16G  1.6G  15G  10% /
/dev/nvme1n1     30G   33M  30G   1% /data
...
```

### Exemplo: estender o sistema de arquivos de volumes do EBS

Para este exemplo, suponha que você tenha redimensionado o volume de inicialização de uma instância, como uma instância T2, de 8 GB para 16 GB e um volume adicional de 8 GB para 30 GB. Use o procedimento a seguir para estender o sistema de arquivos dos volumes redimensionados.

#### Como estender o sistema de arquivos de volumes do EBS

1. [Conecte-se à sua instância \(p. 535\)](#).
2. Para verificar o sistema de arquivos em uso para cada volume, use o comando df -hT.

```
[ec2-user ~]$ df -hT
```

O exemplo de saída a seguir mostra uma instância que tem um volume de inicialização com um sistema de arquivos ext4 e um volume adicional com um sistema de arquivos XFS.

```
[ec2-user ~]$ df -hT
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/xvda1      ext4  8.0G  1.9G  6.2G  24% /
/dev/xvdf1      xfs   8.0G   45M  8.0G   1% /data
...
```

3. Para verificar se o volume tem uma partição que deve ser estendida, use o comando lsblk para exibir informações sobre os dispositivos de blocos anexados à instância.

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda     202:0    0   16G  0 disk
##xvda1  202:1    0    8G  0 part /
xvdf     202:80   0   30G  0 disk
##xvdf1  202:81   0    8G  0 part /data
```

Este exemplo de saída mostra o seguinte:

- O volume raiz, /dev/xvda, tem uma partição, /dev/xvda1. Embora o tamanho do volume seja de 16 GB, o tamanho da partição ainda é de 8 GB e deve ser estendido.
  - O volume /dev/xvdf tem uma partição, /dev/xvdf1. Embora o tamanho do volume seja de 30 GB, o tamanho da partição ainda é de 8 GB e deve ser estendido.
4. Para volumes que têm uma partição, como os volumes mostrados na etapa anterior, use o comando growpart para estender a partição. Observe que há um espaço entre o nome do dispositivo e o número da partição.

```
[ec2-user ~]$ sudo growpart /dev/xvda 1
[ec2-user ~]$ sudo growpart /dev/xvdf 1
```

5. (Opcional) Use o comando lsblk novamente para verificar se as partições refletem o tamanho do volume aumentado.

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda     202:0    0   16G  0 disk
##xvda1  202:1    0   16G  0 part /
xvdf     202:80   0   30G  0 disk
##xvdf1  202:81   0   30G  0 part /data
```

6. Use o comando df -h para verificar o tamanho do sistema de arquivos de cada volume. Neste exemplo de saída, ambos os sistemas de arquivos refletem o tamanho original do volume, 8 GB.

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1      8.0G  1.9G  6.2G  24% /
/dev/xvdf1      8.0G   45M  8.0G   1% /data
...
```

7. Para estender o sistema de arquivos em cada volume, use o comando correto para seu sistema de arquivos, como segue:

- [Volumes do XFS] Use o comando xfs\_growfs para estender o sistema de arquivos em cada volume. Neste exemplo, / e /data são os pontos de montagem de volume mostrados na saída de df -h.

```
[ec2-user ~]$ sudo xfs_growfs -d /
[ec2-user ~]$ sudo xfs_growfs -d /data
```

Se as ferramentas do XFS ainda não estiverem instaladas, você poderá instalá-las da seguinte forma.

```
[ec2-user ~]$ sudo yum install xfsprogs
```

- [volumes do ext4] Use o comando resize2fs para estender o sistema de arquivos em cada volume.

```
[ec2-user ~]$ sudo resize2fs /dev/xvda1
[ec2-user ~]$ sudo resize2fs /dev/xvdf1
```

- [Outro sistema de arquivos] Para estender o sistema de arquivos em cada volume, consulte a documentação do sistema de arquivos para obter instruções.

8. (Opcional) Use o comando df -h novamente para verificar se cada sistema de arquivos reflete o tamanho do volume aumentado.

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       16G  1.9G  14G  12% /
/dev/xvdf1       30G   45M  30G   1% /data
...
```

## 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 \(p. 1418\)](#)
- [Requirements \(p. 1420\)](#)
- [Padrão Chave do KMS para criptografia EBS \(p. 1421\)](#)
- [Criptografia por padrão \(p. 1421\)](#)
- [Criptografar recursos do EBS \(p. 1423\)](#)
- [Cenários de criptografia \(p. 1424\)](#)
- [Configurar padrões de criptografia usando a API e a CLI \(p. 1429\)](#)

## 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 \(p. 204\)](#) e nos seguintes tipos de instância da [geração anterior \(p. 208\)](#): 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 \(p. 1423\)](#).

Por padrão, a criptografia não tem efeito sobre volumes ou snapshots do EBS existentes.

## Considerations

- 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 \(p. 1420\)](#).
- 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 \(p. 1421\)](#) 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 \(p. 1427\)](#).

### 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. \(p. 1274\)](#).

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 \(p. 1319\)](#).

## 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. \(p. 1274\)](#) e [Copiar um snapshot do Amazon EBS. \(p. 1313\)](#).

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 \(criptografia por padrão não habilitada\) \(p. 1425\)](#).

### 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 \(p. 163\)](#).

## 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 \(p. 1421\)](#).

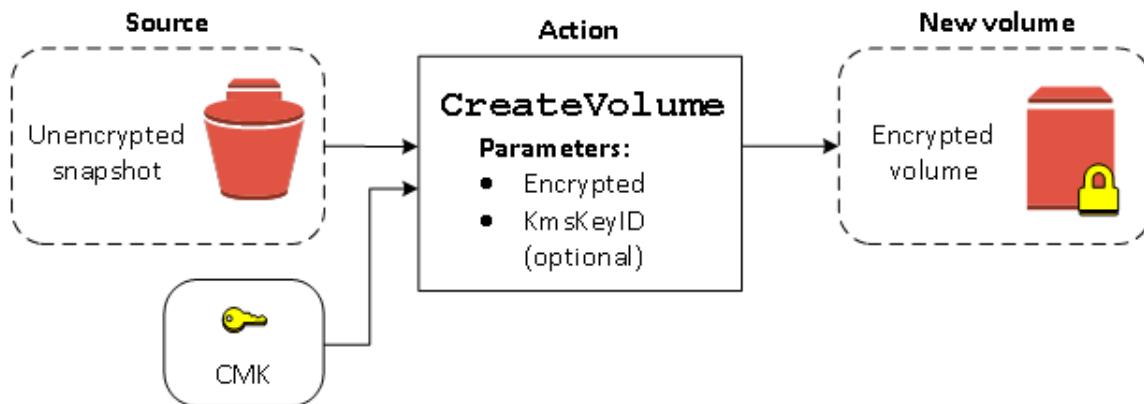
Os exemplos a seguir ilustram como você pode gerenciar o estado de criptografia de seus volumes e snapshots. Para obter uma lista completa de casos de criptografia, consulte a [tabela de resultados de criptografia \(p. 1427\)](#).

### Exemplos

- [Restaurar um volume não criptografado \(criptografia por padrão não habilitada\) \(p. 1424\)](#)
- [Restaurar um volume não criptografado \(criptografia por padrão habilitada\) \(p. 1425\)](#)
- [Copiar um snapshot não criptografado \(criptografia por padrão não habilitada\) \(p. 1425\)](#)
- [Copiar um snapshot não criptografado \(criptografia por padrão habilitada\) \(p. 1425\)](#)
- [Criptografar novamente um volume criptografado \(p. 1426\)](#)
- [Criptografar novamente um snapshot criptografado \(p. 1426\)](#)
- [Migrar dados entre volumes criptografados e não criptografados \(p. 1427\)](#)
- [Resultados da criptografia \(p. 1427\)](#)

### 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.

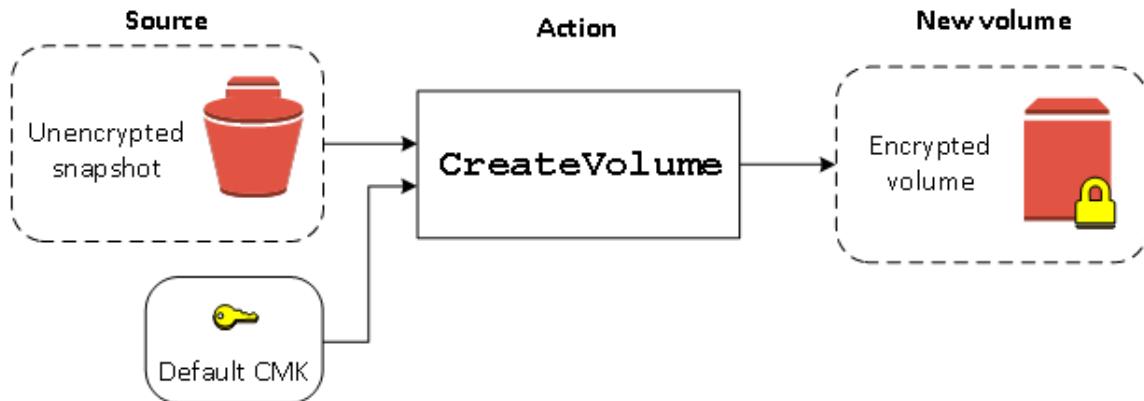


Se você deixar o parâmetro `KmsKeyId` de fora, o volume resultante será criptografado usando a Chave do KMS padrão para a criptografia do EBS. Você deve especificar o ID de uma Chave do KMS para criptografar o volume de uma Chave do KMS diferente.

Para obter mais informações, consulte [Criar um volume a partir de um snapshot \(p. 1275\)](#).

### 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:

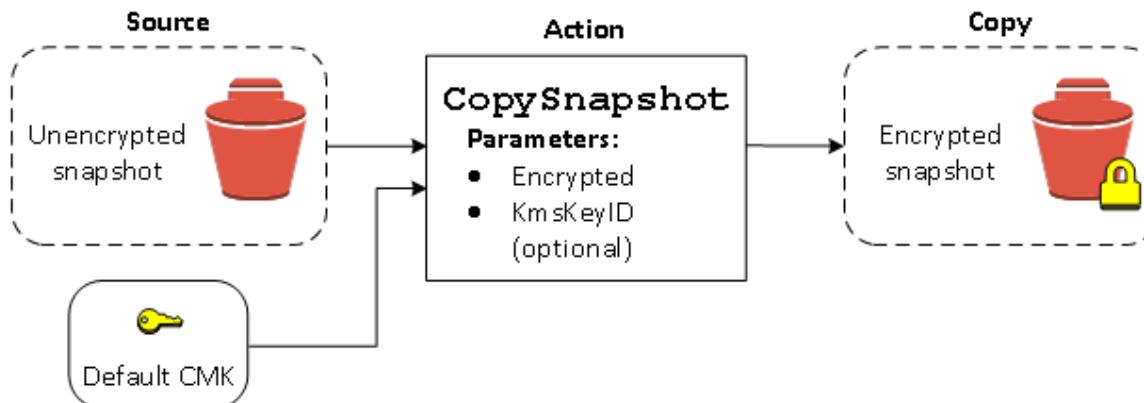


Se quiser criptografar o volume restaurado para uma **Encrypted** simétrica, você deverá fornecer os parâmetros chave gerenciada pelo cliente e **KmsKeyId**, conforme mostrado em [Restaurar um volume não criptografado \(criptografia por padrão não habilitada\) \(p. 1424\)](#).

### 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.

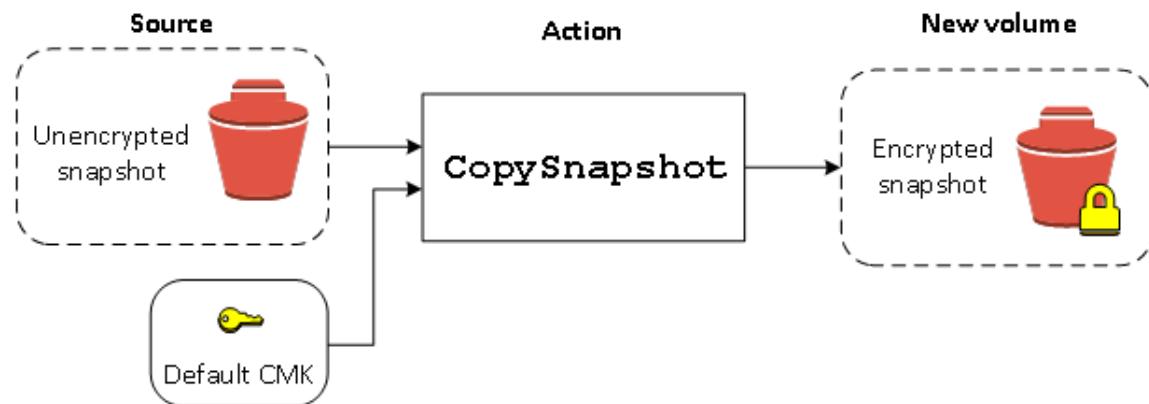
O diagrama a seguir ilustra o processo.



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. \(p. 1313\)](#).

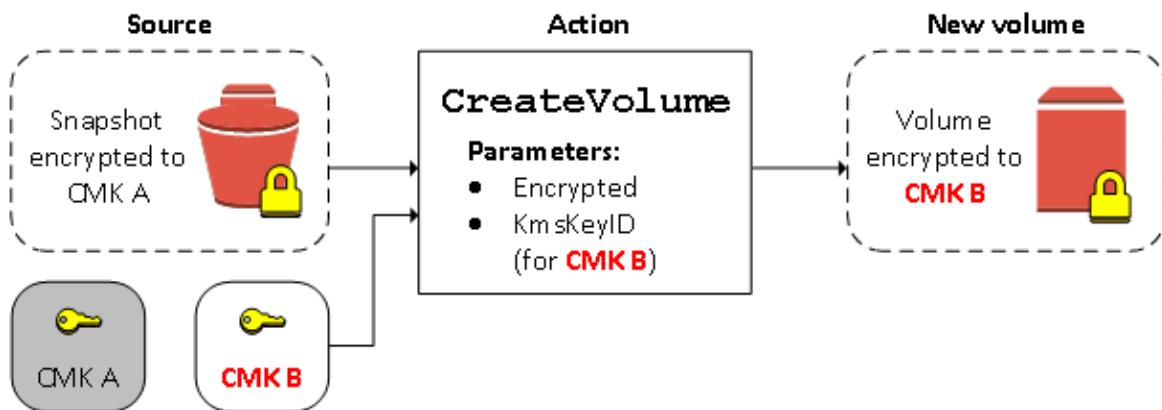
### Copiar um snapshot não criptografado (criptografia por padrão habilitada)

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

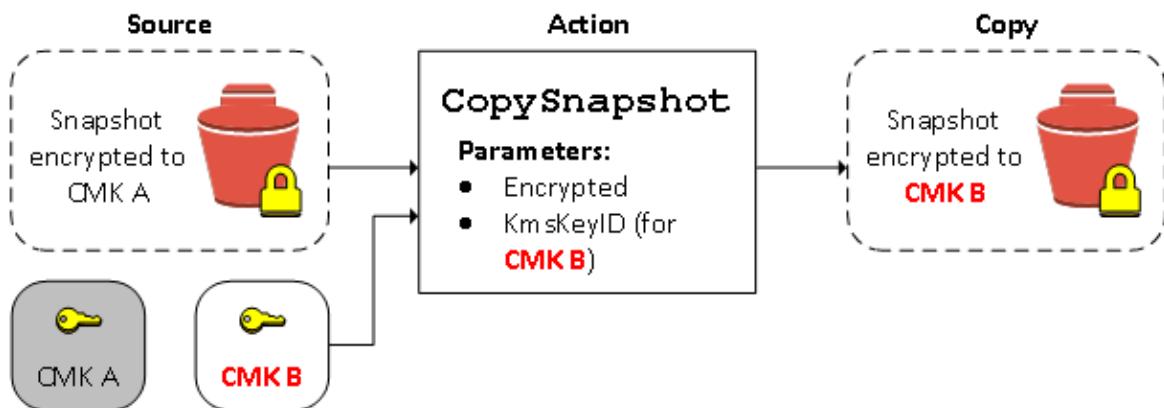
Quando a ação `CreateVolume` opera em um snapshot criptografado, você tem a opção de criptografá-lo novamente com uma Chave do KMS diferente. O diagrama a seguir ilustra o processo. Neste exemplo, você tem duas Chaves do KMS: Chave do KMS A e Chave do KMS B. O snapshot de origem é criptografado pela 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 \(p. 1275\)](#).

#### 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 \(p. 1315\)](#).

### 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 rsync para copiar os dados. No comando a seguir, os dados de origem estão localizados em /mnt/source e o volume de destino está montado em /mnt/destination.

```
[ec2-user ~]$ sudo rsync -avh --progress /mnt/source/ /mnt/destination/
```

### 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	

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Serviços de dados do EBS

			Padrão (nenhuma chave gerenciada pelo cliente especificada)	Personalizado (chave gerenciada pelo cliente especificada)
			gerenciada pelo cliente*	
Sim	Não	Novo volume	Criptografado por chave padrão gerenciada pelo cliente	Criptografado por uma chave gerenciada pelo cliente especificada**
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 gerenciada pelo cliente	N/D
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

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)
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 \(p. 1421\)](#).

\*\* 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

Ação de API	Comando da CLI	Descrição
		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 \(p. 1430\)](#)
- [Estados da restauração rápida de snapshots \(p. 1430\)](#)
- [Créditos de criação de volume \(p. 1431\)](#)
- [Gerenciar a restauração rápida de snapshots \(p. 1431\)](#)
- [Exibir snapshots com restauração rápida de snapshot ativada \(p. 1432\)](#)
- [Exibir volumes restaurados usando restauração rápida de snapshot \(p. 1433\)](#)
- [Monitorar a restauração rápida de snapshot \(p. 1434\)](#)
- [Definição de preço e cobrança \(p. 1434\)](#)

## 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 \(p. 1482\)](#).

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 descompartilha-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 \(p. 1491\)](#).

## 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 Linux

Os volumes do EBS são expostos como dispositivos de blocos NVMe em instâncias criadas no [sistema Nitro \(p. 210\)](#). Os nomes dos dispositivos são `/dev/nvme0n1`, `/dev/nvme1n1` e assim por diante. 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`). O driver do dispositivo de blocos pode atribuir nomes de dispositivos NVMe em uma ordem diferente da especificada para os volumes no mapeamento de dispositivos de blocos.

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 \(p. 1434\)](#)
- [Identificar o dispositivo EBS \(p. 1435\)](#)
- [Trabalhar com volumes de NVMe do EBS \(p. 1437\)](#)
- [Tempo limite de operação de E/S \(p. 1438\)](#)

## Instalar ou atualizar o driver NVMe

Para acessar os volumes de NVMe, os drivers de NVMe devem ser instalados. As instâncias podem ser compatíveis com volumes NVMe do EBS, com volumes de armazenamento de instâncias NVMe, com os dois tipos de volumes de NVMe ou com nenhum volume de NVMe. Para obter mais informações, consulte [Resumo de recursos de redes e armazenamento \(p. 211\)](#).

As seguintes AMIs incluem os drivers NVMe necessários:

- Amazon Linux 2

- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (com kernel `linux-aws`) ou posterior
- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior

Para obter mais informações sobre drivers NVMe em instâncias Windows, consulte [Amazon EBS e NVMe em instâncias Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Como confirmar se a instância tem o driver NVMe

É possível confirmar que sua instância tem o driver NVMe e verificar a versão do driver usando o comando a seguir. Se a instância tiver o driver NVMe, o comando retornará informações sobre o driver.

```
$ modinfo nvme
```

Como atualizar o driver NVMe

Se sua instância tiver o driver NVMe, você poderá atualizar o driver para a versão mais recente usando o procedimento a seguir.

1. Conecte-se à sua instância.
2. Atualize o cache de pacotes para obter as atualizações de pacotes necessárias da seguinte forma:

- Para Amazon Linux 2, Amazon Linux, CentOS e Red Hat Enterprise Linux:

```
[ec2-user ~]$ sudo yum update -y
```

- Para Ubuntu e Debian:

```
[ec2-user ~]$ sudo apt-get update -y
```

3. Ubuntu 16.04 ou posterior incluem o pacote `linux-aws`, que contém os drivers NVMe e ENA exigidos pelas instâncias baseadas em Nitro. Atualize o pacote `linux-aws` para receber a versão mais recente da seguinte forma:

```
[ec2-user ~]$ sudo apt-get install --only-upgrade -y linux-aws
```

Para o Ubuntu 14.04, você pode instalar o pacote mais recente `linux-aws` da seguinte maneira:

```
[ec2-user ~]$ sudo apt-get install linux-aws
```

4. Reinicialize sua instância para carregar a versão mais recente do kernel.

```
sudo reboot
```

5. Reconecte-se à sua instância depois de reinicializá-la.

## 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. No Linux, os nomes de dispositivos NVMe seguem o padrão `/dev/nvme<x>n<y>`, em que `<x>` é a ordem de enumeração e, para o EBS, `<y>` é igual a 1. Ocasionalmente, os dispositivos podem responder à descoberta em uma ordem diferente em inicializações subsequentes da instância, o que faz com que o nome do dispositivo seja alterado. 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.

Recomendamos que você use identificadores estáveis para seus volumes do EBS em sua instância, como um dos seguintes:

- Para instâncias baseadas em Nitro, os mapeamentos de dispositivos de blocos especificados no console do Amazon EC2, quando você está anexando um volume do EBS ou durante chamadas à API `AttachVolume` ou `RunInstances`, são capturados no campo de dados específico ao fornecedor da identificação do controlador NVMe. Com as AMIs do Amazon Linux posteriores à versão 2017.09.01, fornecemos uma regra udev que lê esses dados e cria um link simbólico para o mapeamento de dispositivos de blocos.
- O ID do volume do EBS e o ponto de montagem são estáveis entre as alterações de estado da instância. O nome do dispositivo NVMe pode mudar, dependendo da ordem em que os dispositivos respondem durante a inicialização da instância. Recomendamos usar o ID do volume do EBS e o ponto de montagem para a identificação consistente do dispositivo.
- Os volumes do EBS do NVMe têm o ID do volume do EBS definido como o número de série na identificação do dispositivo. Use o comando `lsblk -o +SERIAL` para listar o número de série.
- O formato de nome do dispositivo NVMe pode variar dependendo se o volume do EBS foi anexado durante ou após o lançamento da instância. Os nomes de dispositivos NVMe para volumes anexados após o lançamento da instância incluem o prefixo `/dev/`, enquanto os nomes de dispositivos NVMe para volumes anexados durante o lançamento da instância não incluem o prefixo `/dev/`. Se você estiver usando um Amazon Linux ou FreeBSD AMI, use o comando `sudo ebsnvme-id /dev/nvme0n1 -u` para ter um nome de dispositivo NVMe consistente. Para outras distribuições, use o `sudo ebsnvme-id /dev/nvme0n1 -u` para determinar o nome do dispositivo NVMe.
- Quando um dispositivo é formatado, um UUID é gerado que persiste durante a vida do sistema de arquivos. Um rótulo de dispositivo pode ser especificado ao mesmo tempo. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Linux \(p. 1283\)](#) e [Inicialização a partir do volume errado \(p. 1612\)](#).

#### Amazon Linux AMIs

Com a AMI do Amazon Linux 2017.09.01 ou posterior (incluindo o Amazon Linux 2), você pode executar o comando `ebsnvme-id` da seguinte forma para mapear o nome do dispositivo NVMe para um ID de volume e nome de dispositivo:

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/`.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme0n1
Volume ID: vol-01324f611e2463981
sda
```

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/`.

```
[ec2-user ~]$ sudo /sbin/ebsnvme-id /dev/nvme1n1
Volume ID: vol-064784f1011136656
/dev/sdf
```

Amazon Linux também cria um link simbólico do nome do dispositivo no mapeamento de dispositivos de blocos (por exemplo, `/dev/sdf`), para o nome do dispositivo NVMe.

#### AMIs do FreeBSD

Começando com o FreeBSD 12.2-RELEASE, você pode executar o comando `ebsnvme-id` conforme mostrado acima. Passe o nome do dispositivo NVMe (por exemplo, `nvme0`) ou o dispositivo de disco (por exemplo, `nvd0` ou `nda0`). O FreeBSD também cria links simbólicos para os dispositivos de disco (por exemplo, `/dev/aws/disk/ebs/volume_id`).

#### Outras AMIs em Linux

Com uma versão do kernel de 4.2 ou posterior, você pode executar o comando `nvme id-ctrl` da seguinte forma para mapear um dispositivo NVMe para um ID de volume. Primeiro, instale o pacote da linha de comando do NVMe, `nvme-cli`, usando as ferramentas de gerenciamento de pacotes para sua distribuição do Linux. Para obter instruções de download e instalação de outras distribuições, consulte a documentação específica para sua distribuição.

O exemplo a seguir obtém o ID do volume e o nome do dispositivo NVMe para um volume que foi anexado durante o lançamento da instância. Observe que o nome do dispositivo NVMe não inclui o prefixo `/dev/`. O nome do dispositivo está disponível por meio da extensão específica ao fornecedor do controlador NVMe (384:4095 bytes da identificação do controlador):

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme0n1
NVME Identify Controller:
vid      : 0x1d0f
ssvid    : 0x1d0f
sn      : vol01234567890abcdef
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "sda..."
```

O exemplo a seguir obtém o ID do volume e o nome do dispositivo NVMe para um volume que foi anexado após o lançamento da instância. Observe que o nome do dispositivo NVMe inclui o prefixo `/dev/`.

```
[ec2-user ~]$ sudo nvme id-ctrl -v /dev/nvme1n1
NVME Identify Controller:
vid      : 0x1d0f
ssvid    : 0x1d0f
sn      : volabcdef01234567890
mn      : Amazon Elastic Block Store
...
0000: 2f 64 65 76 2f 73 64 6a 20 20 20 20 20 20 20 20 "/dev/sdf..."
```

O comando `lsblk` lista dispositivos disponíveis e seus pontos de montagem (se aplicável). Isso ajuda você a determinar o nome correto do dispositivo a ser usado. Neste exemplo, `/dev/nvme0n1p1` é montado como o dispositivo raiz e `/dev/nvme1n1` é anexado mas não montado.

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme1n1   259:3    0 100G  0 disk
nvme0n1   259:0    0   8G  0 disk
  nvme0n1p1 259:1    0   8G  0 part /
  nvme0n1p128 259:2   0   1M  0 part
```

## Trabalhar com volumes de NVMe do EBS

Para formatar e montar um volume de NVMe do EBS, consulte [Disponibilizar um volume do Amazon EBS para uso no Linux \(p. 1283\)](#).

Se você estiver usando o kernel Linux 4.2 ou posterior, qualquer alteração que você fizer no tamanho do volume de um volume de NVMe do EBS será automaticamente refletida na instância. Para os kernels do Linux mais antigos, talvez seja necessário desanexar e anexar o volume do EBS ou reiniciar a instância para que a alteração de tamanho seja refletida. Com o kernel 3.19 ou posterior do Linux, você pode usar o comando hdparm da seguinte forma para forçar uma nova varredura do dispositivo NVMe:

```
[ec2-user ~]$ sudo hdparm -z /dev/nvme1n1
```

Quando você desanexa um volume de NVMe do EBS, a instância não tem a oportunidade de liberar os caches ou metadados do sistema de arquivos antes de desanexar o volume. Portanto, antes de desanexar um volume de NVMe do EBS, você deverá sincronizá-lo e desmontá-lo. Se o volume não for desanexado, tente o comando `force-detach`, conforme descrito em [Desanexar um volume do Amazon EBS de uma instância Linux \(p. 1300\)](#).

## Tempo limite de operação de E/S

Os volumes do EBS anexados a instâncias baseadas em Nitro usam o driver NVMe padrão fornecido pelo sistema operacional. A maioria dos sistemas operacionais especifica um tempo limite para as operações de E/S enviadas aos dispositivos NVMe. O tempo limite padrão é de 30 segundos e pode ser alterado usando o parâmetro de inicialização `nvme_core.io_timeout`. Para a maioria dos kernels do Linux anteriores à versão 4.6, esse parâmetro é `nvme.io_timeout`.

Se a latência de E/S exceder o valor desse parâmetro de tempo limite, o driver NVMe do Linux falhará na E/S e retornará um erro ao sistema de arquivos ou à aplicação. Dependendo da operação de E/S, seu sistema de arquivos ou aplicação poderá tentar o erro novamente. Em alguns casos, o sistema de arquivos pode ser remontado como somente leitura.

Para obter uma experiência semelhante à dos volumes do EBS anexados às instâncias do Xen, recomendamos que você configure `nvme_core.io_timeout` como o maior valor possível. Para os kernels atuais, o máximo é 4294967295, enquanto para os kernels anteriores o máximo é 255. Dependendo da versão do Linux, o tempo limite pode já estar definido como o máximo valor possível. Por exemplo, o tempo limite é definido como 4294967295 por padrão para a AMI do Amazon Linux 2017.09.01 e posterior.

É possível verificar o valor máximo de sua distribuição Linux gravando um valor mais alto que o máximo sugerido para `/sys/module/nvme_core/parameters/io_timeout` e verificando se ocorre o erro Resultado numérico fora do intervalo ao tentar salvar o arquivo.

## 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 \(p. 1253\)](#).

### Tópicos

- [Tipos de instâncias compatíveis \(p. 1439\)](#)
- [Obtenha a máxima performance \(p. 1457\)](#)

- [Exibir tipos de instâncias compatíveis com a otimização do EBS \(p. 1458\)](#)
- [Habilitação da otimização do EBS na execução \(p. 1459\)](#)
- [Habilitar a otimização do EBS para uma instância existente \(p. 1459\)](#)

## 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 \(p. 1458\)](#).

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)
a1.medium *	3.500	437,5	20.000
a1.large *	3.500	437,5	20.000
a1.xlarge *	3.500	437,5	20.000
a1.2xlarge *	3.500	437,5	20.000
a1.4xlarge	3.500	437,5	20.000
a1.metal	3.500	437,5	20.000
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
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
c6g.medium *	4.750	593,75	20.000
c6g.large *	4.750	593,75	20.000
c6g.xlarge *	4.750	593,75	20.000
c6g.2xlarge *	4.750	593,75	20.000
c6g.4xlarge	4.750	593,75	20.000
c6g.8xlarge	9.500	1.187,5	40.000
c6g.12xlarge	14.250	1.781,25	50.000
c6g.16xlarge	19.000	2.375	80.000
c6g.metal	19.000	2.375	80.000
c6gd.medium *	4.750	593,75	20.000
c6gd.large *	4.750	593,75	20.000
c6gd.xlarge *	4.750	593,75	20.000
c6gd.2xlarge *	4.750	593,75	20.000
c6gd.4xlarge	4.750	593,75	20.000
c6gd.8xlarge	9.500	1.187,5	40.000
c6gd.12xlarge	14.250	1.781,25	50.000
c6gd.16xlarge	19.000	2.375	80.000
c6gd.metal	19.000	2.375	80.000
c6gn.medium *	9.500	1.187,5	40.000
c6gn.large *	9.500	1.187,5	40.000
c6gn.xlarge *	9.500	1.187,5	40.000
c6gn.2xlarge *	9.500	1.187,5	40.000
c6gn.4xlarge	9.500	1.187,5	40.000

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
c6gn.8xlarge	19.000	2.375	80.000
c6gn.12xlarge	28.500	3.562,5	120.000
c6gn.16xlarge	38.000	4.750	160.000
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
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
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
inf1.xlarge *	4.750	593,75	20.000
inf1.2xlarge *	4.750	593,75	20.000
inf1.6xlarge	4.750	593,75	20.000
inf1.24xlarge	19.000	2.375	80.000
m4.large	450	56,25	3.600
m4.xlarge	750	93,75	6.000

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
m5zn.6xlarge	9.500	1187,5	40.000
m5zn.12xlarge	19.000	2.375	80.000
m5zn.metal	19.000	2.375	80.000
m6g.medium *	4.750	593,75	20.000
m6g.large *	4.750	593,75	20.000
m6g.xlarge *	4.750	593,75	20.000
m6g.2xlarge *	4.750	593,75	20.000
m6g.4xlarge	4.750	593,75	20.000
m6g.8xlarge	9.500	1.187,5	40.000
m6g.12xlarge	14.250	1.781,25	50.000
m6g.16xlarge	19.000	2.375	80.000
m6g.metal	19.000	2.375	80.000
m6gd.medium *	4.750	593,75	20.000
m6gd.large *	4.750	593,75	20.000
m6gd.xlarge *	4.750	593,75	20.000
m6gd.2xlarge *	4.750	593,75	20.000
m6gd.4xlarge	4.750	593,75	20.000
m6gd.8xlarge	9.500	1.187,5	40.000
m6gd.12xlarge	14.250	1.781,25	50.000
m6gd.16xlarge	19.000	2.375	80.000
m6gd.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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
mac1.metal	8.000	1.000	55.000
p2.xlarge	750	93,75	6.000
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
p4d.2xlarge	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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
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
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
r5dn.2xlarge *	4.750	593,75	18.750
r5dn.4xlarge	4.750	593,75	18.750
r5dn.8xlarge	6.800	850	30.000
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
r6g.medium *	4.750	593,75	20.000
r6g.large *	4.750	593,75	20.000
r6g.xlarge *	4.750	593,75	20.000
r6g.2xlarge *	4.750	593,75	20.000
r6g.4xlarge	4.750	593,75	20.000
r6g.8xlarge	9.500	1.187,5	40.000
r6g.12xlarge	14.250	1.781,25	50.000
r6g.16xlarge	19.000	2.375	80.000
r6g.metal	19.000	2.375	80.000
r6gd.medium *	4.750	593,75	20.000
r6gd.large *	4.750	593,75	20.000
r6gd.xlarge *	4.750	593,75	20.000
r6gd.2xlarge *	4.750	593,75	20.000
r6gd.4xlarge	4.750	593,75	20.000

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
r6gd.8xlarge	9.500	1.187,5	40.000
r6gd.12xlarge	14.250	1.781,25	50.000
r6gd.16xlarge	19.000	2.375	80.000
r6gd.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
t4g.nano *	2.606	325,75	11.800
t4g.micro *	2.606	325,75	11.800
t4g.small *	2.606	325,75	11.800
t4g.medium *	2.606	325,75	11.800
t4g.large *	3.475	434,37	15.700
t4g.xlarge *	3.475	434,37	15.700
t4g.2xlarge *	3.475	434,37	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
u-9tb1.112xlarge	38.000	4.750	160.000
u-9tb1.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-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
x2gd.medium *	4.750	593,75	20.000
x2gd.large *	4.750	593,75	20.000
x2gd.xlarge *	4.750	593,75	20.000
x2gd.2xlarge *	4.750	593,75	20.000
x2gd.4xlarge	4.750	593,75	20.000
x2gd.8xlarge	9.500	1.187,5	40.000
x2gd.12xlarge	14.250	1.781,25	60.000
x2gd.16xlarge	19.000	2.375	80.000
x2gd.metal	19.000	2.375	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)
a1.medium	300	37,5	2.500
a1.large	525	65,625	4.000
a1.xlarge	800	100	6.000
a1.2xlarge	1.750	218,75	10.000
c5.large	650	81,25	4.000
c5.xlarge	1.150	143,75	6.000
c5.2xlarge	2.300	287,5	10.000
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
c6g.medium	315	39,375	2.500
c6g.large	630	78,75	3.600
c6g.xlarge	1.188	148,5	6.000
c6g.2xlarge	2.375	296,875	12.000
c6gd.medium	315	39,375	2.500
c6gd.large	630	78,75	3.600
c6gd.xlarge	1.188	148,5	6.000

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
c6gd.2xlarge	2.375	296,875	12.000
c6gn.medium	760	95	2.500
c6gn.large	1.235	154.375	5.000
c6gn.xlarge	1.900	237,5	10.000
c6gn.2xlarge	4.750	593,75	20.000
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
inf1.xlarge	1.190	148,75	4.000
inf1.2xlarge	1.190	148,75	6.000
m5.large	650	81,25	3.600
m5.xlarge	1.150	143,75	6.000
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
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
m6g.medium	315	39,375	2.500
m6g.large	630	78,75	3.600
m6g.xlarge	1.188	148,5	6.000
m6g.2xlarge	2.375	296,875	12.000
m6gd.medium	315	39,375	2.500
m6gd.large	630	78,75	3.600
m6gd.xlarge	1.188	148,5	6.000
m6gd.2xlarge	2.375	296,875	12.000
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

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
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)
r5ad.xlarge	1.085	135,63	6.000
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
r6g.medium	315	39,375	2.500
r6g.large	630	78,75	3.600
r6g.xlarge	1.188	148,5	6.000
r6g.2xlarge	2.375	296,875	12.000
r6gd.medium *	315	39,375	2.500
r6gd.large *	630	78,75	3.600
r6gd.xlarge *	1.188	148,5	6.000
r6gd.2xlarge *	2.375	296,875	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

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)
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
t4g.nano	32	4	250
t4g.micro	64	8	500
t4g.small	128	16	1.000
t4g.medium	256	32	2.000
t4g.large	512	64	4.000
t4g.xlarge	1.024	128	4.000
t4g.2xlarge	2.048	256	4.000
x2gd.medium	315	39,375	2.500
x2gd.large	630	78,75	3.600
x2gd.xlarge	1.188	148,5	6.000
x2gd.2xlarge	2.375	296,875	12.000
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 \(p. 1458\)](#).

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 \(p. 872\)](#).

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 pesados 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 pesados 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](#).

## Considerations

- As instâncias G4dn, I3en, Inf1, 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.

```
$ 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=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.

```
$ 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 Linux

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 Linux](#).

#### Tópicos

- [Dicas de performance do Amazon EBS \(p. 1461\)](#)
- [Características e monitoramento de E/S \(p. 1463\)](#)
- [Inicializar volumes de Amazon EBS \(p. 1466\)](#)
- [Configuração RAID no Linux \(p. 1468\)](#)
- [Comparar volumes do EBS \(p. 1472\)](#)

## 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 \(p. 1438\)](#).

### 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 \(p. 1463\)](#).

### 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. Para obter mais informações, consulte [Comparar volumes do EBS \(p. 1472\)](#).

### 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 \(p. 1466\)](#).
- 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 \(p. 1430\)](#).

## 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 \(p. 1253\)](#).

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 \(p. 1463\)](#).

## Aumentar a leitura antecipada para workloads com muita leitura e alta taxa de transferência em st1 e em sc1

Algumas workloads têm muita leitura e acessam o dispositivo de blocos pelo cache da página do sistema operacional (por exemplo, de um sistema de arquivos). Nesse caso, para alcançar a taxa de transferência máxima, recomendamos que você defina a configuração de leitura antecipada como 1 MiB. Essa é uma configuração de dispositivo por bloco que somente deve ser aplicada aos volumes de HDD.

Para examinar o valor atual de leitura antecipada para os dispositivos de blocos, use o seguinte comando:

```
[ec2-user ~]$ sudo blockdev --report /dev/<device>
```

As informações do dispositivo de blocos são retornadas neste formato:

RO	RA	SSZ	BSZ	StartSec	Size	Device
rw	256	512	4096	4096	8587820544	/dev/<device>

O dispositivo mostrado relata um valor de leitura antecipada de 256 (o padrão). Multiplique esse número pelo tamanho do setor (512 bytes) para obter o tamanho de buffer de leitura antecipada, que nesse caso é 128 KiB. Para configurar o valor de buffer de 1 MiB, use o seguinte comando:

```
[ec2-user ~]$ sudo blockdev --setra 2048 /dev/<device>
```

Verifique se a configuração de leitura antecipada agora exibe 2.048 executando o primeiro comando novamente.

Use essa configuração somente quando sua workload consistir em grandes E/S sequenciais. Se consistir principalmente em pequenas E/S aleatórias, essa configuração acabará reduzindo a performance. Em geral, se sua workload consiste principalmente em operações de E/S pequenas ou aleatórias, você deve avaliar a possibilidade de usar um volume SSD de uso geral (gp2 e gp3) em vez de um volume st1 ou sc1.

## Usar um kernel do Linux moderno

Use um kernel do Linux moderno com suporte para descritores indiretos. Qualquer kernel do Linux versão 3.8 e posterior tem esse suporte, bem como qualquer instância do EC2 da geração atual. Se o tamanho médio de E/S for igual ou próximo a 44 KiB, você poderá usar uma instância ou um kernel sem

suporte para descritores indiretos. Para obter informações sobre como derivar o tamanho médio de E/S de métricas do Amazon CloudWatch, consulte [Características e monitoramento de E/S \(p. 1463\)](#).

Para alcançar a taxa de transferência máxima em volumes `st1` ou `sc1`, recomendamos aplicar um valor de 256 ao parâmetro `xen_blkfront.max` (para versões de kernel do Linux abaixo de 4.6) ou o parâmetro `xen_blkfront.max_indirect_segments` (para a versão de kernel do Linux 4.6 e acima). O parâmetro apropriado pode ser definido na linha de comando de inicialização do sistema operacional.

Por exemplo, em uma AMI do Amazon Linux com um kernel mais antigo, você pode adicioná-lo ao final da linha de kernel na configuração de GRUB encontrada em `/boot/grub/menu.lst`:

```
kernel /boot/vmlinuz-4.4.5-15.26.amzn1.x86_64 root=LABEL=/ console=ttyS0
xen_blkfront.max=256
```

Para um kernel mais recente, o comando será semelhante ao seguinte:

```
kernel /boot/vmlinuz-4.9.20-11.31.amzn1.x86_64 root=LABEL=/ console=tty1 console=ttyS0
xen_blkfront.max_indirect_segments=256
```

Reinicialize sua instância para que essa configuração seja implementada.

Para obter mais informações, consulte [Configuring GRUB \(p. 193\)](#). Outras distribuições do Linux, especialmente aquelas que não usam o carregador de inicialização de GRUB, podem exigir uma abordagem diferente para ajustar os parâmetros de kernel.

Para obter mais informações sobre as características de E/S do EBS, consulte a apresentação re:Invent [Amazon EBS: Como projetar visando a performance](#) neste tópico.

## 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 Linux \(p. 1468\)](#).

## 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 \(p. 1292\)](#).

## 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 \(p. 1464\)](#)
- [Comprimento e latência da fila de volume \(p. 1465\)](#)
- [Limites de taxa de transferência de tamanho e volume de E/S \(p. 1465\)](#)

- [Monitorar as características de E/S usando o CloudWatch \(p. 1466\)](#)
- [Recursos relacionados \(p. 1466\)](#)

## 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 de 128 KiB em uma única operação de E/S de 1.024 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 \(p. 1253\)](#).

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 \(p. 1438\)](#). 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 \(p. 1478\)](#) 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 \(p. 1477\)](#) e [Métricas do Amazon EBS para instâncias baseadas em Nitro \(p. 880\)](#).

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](#).

## Iniciar 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 obtido 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 \(p. 1292\)](#).

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 Linux \(p. 1467\)](#).
- 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 \(p. 1430\)](#).

## Inicializar volumes de Amazon EBS no Linux

Os volumes vazios do EBS recebem a performance máxima no momento em que são disponibilizados e não requerem inicialização (antes conhecida como pré-aquecimento). Para volumes que foram criados de snapshots, use os utilitários dd ou fio para ler todos os blocos em um volume. Todos os dados existentes no volume serão preservados.

Para obter informações sobre como inicializar volumes do Amazon EBS no Windows, consulte [Inicializar volumes do Amazon EBS no Windows](#).

### Como inicializar um volume criado de um snapshot no Linux

1. Anexe o volume recentemente restaurado à sua instância do Linux.
2. Use o comando lsblk para relacionar os dispositivos de blocos em sua instância.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
xvdf  202:80   0  30G  0 disk 
xvda1 202:1    0   8G  0 disk /
```

Aqui você pode ver que o volume novo /dev/xvdf, está anexado, mas não montado (porque não há caminho listado na coluna MOUNTPOINT).

3. Use os utilitários dd ou fio para ler todos os blocos do dispositivo. O comando dd é instalado por padrão em sistemas Linux, mas fio é consideravelmente mais rápido porque permite leituras encadeadas várias vezes.

**Note**

Essa etapa pode levar 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.

[dd] O parâmetro if (arquivo de entrada) deve ser configurado na unidade que você deseja inicializar. O parâmetro of (arquivo de saída) deve ser definido no dispositivo virtual nulo do Linux, /dev/null.

O parâmetro `bs` define o tamanho do bloco da operação de leitura. Para a performance ideal, ele deve ser definido como 1 MB.

**Important**

O uso incorreto de dd pode destruir facilmente os dados de um volume. Não deixe de seguir precisamente o comando de exemplo abaixo. Somente o parâmetro `if=/dev/xvdf` irá variar dependendo do nome do dispositivo que você está lendo.

```
[ec2-user ~]$ sudo dd if=/dev/xvdf of=/dev/null bs=1M
```

[fio] Se o fio estiver instalado em seu sistema, use o seguinte comando para inicializar seu volume. O parâmetro `--filename` (arquivo de entrada) deve ser configurado na unidade que você deseja inicializar.

```
[ec2-user ~]$ sudo fio --filename=/dev/xvdf --rw=read --bs=128k --iodepth=32 --  
ioengine=libaio --direct=1 --name=volume-initialize
```

Use o comando a seguir para instalar o fio em Amazon Linux:

```
sudo yum install -y fio
```

Para instalar fio no Ubuntu, use o seguinte comando:

```
sudo apt-get install -y fio
```

Quando a operação for concluída, você verá um relatório da operação de leitura. Seu volume agora está pronto para uso. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Linux \(p. 1283\)](#).

## Configuração RAID no Linux

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. O Grub, geralmente, é instalado em apenas um dispositivo em uma matriz RAID, e se um dos dispositivos espelhados falhar, talvez não seja possível inicializar o sistema operacional.

Se você precisar criar uma matriz RAID em uma instância do Windows, consulte [Configuração de RAID no Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

### Tópicos

- [Opções de configuração de RAID \(p. 1469\)](#)
- [Criar uma matriz RAID 0 no Linux \(p. 1469\)](#)

- [Criar snapshots de volumes em uma matriz RAID \(p. 1472\)](#)

## Opções 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, criariam 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 Linux

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 uma matriz de RAID 0. Você pode obter instruções sobre instâncias do Windows em [Create a RAID 0 array on Windows](#) (Criar uma matriz RAID 0 no Windows) no Guia do usuário do Amazon EC2 para instâncias do Windows.

Para criar uma matriz de RAID 0 no Linux

1. Crie os volumes do Amazon EBS para sua matriz. Para obter mais informações, consulte [Crie um volume do Amazon EBS. \(p. 1274\)](#).

### 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. Para obter mais informações, consulte [Instâncias otimizadas para Amazon EBS \(p. 1438\)](#).

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 \(p. 1277\)](#).
3. Use o comando mdadm para criar um dispositivo RAID lógico dos volumes do Amazon EBS anexados recentemente. Substitua o número de volumes em sua matriz por `number_of_volumes` e os nomes

dos dispositivos para cada volume na matriz (como `/dev/xvdf`) por `device_name`. Você também pode substituir `MY_RAID` pelo seu próprio nome exclusivo para a matriz.

Note

Você pode relacionar os dispositivos em sua instância com o comando `lsblk` para encontrar os nomes dos dispositivos.

Para criar uma matriz de RAID 0, execute o seguinte comando (observe a opção `--level=0` para distribuir a matriz):

```
[ec2-user ~]$ sudo mdadm --create --verbose /dev/md0 --level=0 --name=MY_RAID --raid-devices=number_of_volumes device_name1 device_name2
```

- Reserve tempo para a matriz de RAID ser inicializada e sincronizada. Você pode acompanhar o progresso dessas operações com o seguinte comando:

```
[ec2-user ~]$ sudo cat /proc/mdstat
```

A seguir está um exemplo de saída:

```
Personalities : [raid0]
md0 : active raid0 xvdc[1] xvdb[0]
      41910272 blocks super 1.2 512k chunks

unused devices: <none>
```

Em geral, você pode exibir informações detalhadas sobre sua matriz de RAID com o seguinte comando:

```
[ec2-user ~]$ sudo mdadm --detail /dev/md0
```

A seguir está um exemplo de saída:

```
/dev/md0:
      Version : 1.2
      Creation Time : Wed May 19 11:12:56 2021
      Raid Level : raid0
      Array Size : 41910272 (39.97 GiB 42.92 GB)
      Raid Devices : 2
      Total Devices : 2
      Persistence : Superblock is persistent

      Update Time : Wed May 19 11:12:56 2021
      State : clean
      Active Devices : 2
      Working Devices : 2
      Failed Devices : 0
      Spare Devices : 0

      Chunk Size : 512K

      Consistency Policy : none

      Name : MY_RAID
      UUID : 646aa723:db31bbc7:13c43daf:d5c51e0c
      Events : 0

      Number  Major  Minor  RaidDevice State
            0      202      16          0  active sync   /dev/sdb
```

1	202	32	1	active sync	/dev/sdc
---	-----	----	---	-------------	----------

5. Crie um sistema de arquivos em sua matriz de RAID e forneça a esse sistema de arquivos uma identificação para usar quando ao montá-lo posteriormente. Por exemplo, para criar um sistema de arquivos ext4 com a identificação **MY\_RAID**, execute o seguinte comando:

```
[ec2-user ~]$ sudo mkfs.ext4 -L MY_RAID /dev/md0
```

Dependendo dos requisitos da aplicação ou das limitações do sistema operacional, você pode usar um tipo diferente de sistema de arquivos, como ext3 ou XFS (consulte a documentação do sistema de arquivos para saber o comando de criação de sistema de arquivos correspondente).

6. Para garantir que a matriz de RAID seja remontada automaticamente na inicialização, crie um arquivo de configuração para conter informações de RAID:

```
[ec2-user ~]$ sudo mdadm --detail --scan | sudo tee -a /etc/mdadm.conf
```

#### Note

Se você estiver usando uma distribuição do Linux que não seja o Amazon Linux, talvez seja necessário modificar esse comando. Por exemplo, talvez seja necessário colocar o arquivo em outro local, ou talvez seja necessário adicionar o parâmetro `--examine`. Para obter mais informações, execute `man mdadm.conf` em sua instância do Linux.

7. Crie uma nova imagem de ramdisk para pré-carregar corretamente os módulos de dispositivo de bloco para sua nova configuração de RAID:

```
[ec2-user ~]$ sudo dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. Crie um ponto de montagem para sua matriz RAID.

```
[ec2-user ~]$ sudo mkdir -p /mnt/raid
```

9. Finalmente, monte o dispositivo RAID no ponto de montagem que você criou:

```
[ec2-user ~]$ sudo mount LABEL=MY_RAID /mnt/raid
```

O dispositivo RAID agora está pronto para uso.

10. (Opcional) Para montar esse volume do Amazon EBS em cada reinicialização do sistema, adicione uma entrada para o dispositivo ao arquivo `/etc/fstab`.
- a. Crie um backup do seu arquivo `/etc/fstab` para usar se você destruir ou excluir acidentalmente esse arquivo quando for editar.

```
[ec2-user ~]$ sudo cp /etc/fstab /etc/fstab.orig
```

- b. Abra o arquivo `/etc/fstab` usando seu editor de texto favorito, como nano ou vim.
- c. Comente todas as linhas que começam com "UUID=" e, no final do arquivo, adicione uma nova linha para o volume de RAID usando o seguinte formato:

```
device_label mount_point file_system_type fs_mntops fs_freq fs_passno
```

Os três últimos campos dessa linha são as opções de montagem do sistema de arquivos, a frequência de despejo do sistema de arquivos e a ordem das verificações do sistema de arquivos feitas no momento da inicialização. Se você não souber quais valores devem ser, use os valores no exemplo abaixo (`defaults,nofail 0 2`). Para obter mais informações sobre `/etc/`

`fstab`, consulte a página `fstab` do manual (inserindo `man fstab` na linha de comando). Por exemplo, para montar o sistema de arquivos `ext4` no dispositivo com a identificação `MY_RAID` no ponto de montagem `/mnt/raid`, adicione a seguinte entrada a `/etc/fstab`.

Note

Se você pretende inicializar sua instância sem esse volume anexado (por exemplo, para que esse volume possa ser movido entre instâncias diferentes), adicione a opção de montagem `nofail` que permite à instância ser inicializada mesmo se houver erros na montagem do volume. Os derivados de Debian, como o Ubuntu, também devem adicionar a opção de montagem `nobootwait`.

```
LABEL=MY_RAID      /mnt/raid    ext4    defaults,nofail      0      2
```

- d. Depois de adicionar a nova entrada a `/etc/fstab`, você precisa verificar se a sua entrada funciona. Execute o comando `sudo mount -a` para montar todos os sistemas de arquivos em `/etc/fstab`.

```
[ec2-user ~]$ sudo mount -a
```

Se o comando anterior não produzir um erro, o arquivo `/etc/fstab` será válido e o sistema de arquivos será montado automaticamente na próxima inicialização. Se o comando produzir erros, examine-os e tente corrigir seu `/etc/fstab`.

Warning

Erros no arquivo `/etc/fstab` podem impedir a inicialização de um sistema. Não desative um sistema que tenha erros no arquivo `/etc/fstab`.

- e. (Opcional) Se você não souber corrigir os erros no `/etc/fstab`, sempre poderá restaurar seu arquivo `/etc/fstab` de backup com o seguinte comando.

```
[ec2-user ~]$ sudo mv /etc/fstab.orig /etc/fstab
```

## 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 \(p. 1438\)](#).

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 \(p. 1438\)](#).

### 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 \(p. 1253\)](#) e [Crie um volume do Amazon EBS. \(p. 1274\)](#).

Para os testes de exemplo, recomendamos que você crie uma matriz de RAID 0 com 6 volumes, que oferece um alto nível de performance. Como você será cobrado por gigabytes provisionados (e pelo número de IOPS provisionadas para volumes de io1, io2 e gp3), e não pelo número de volumes, não há nenhum custo adicional para criar vários volumes menores e utilizá-los para criar um conjunto de stripes. Se você estiver utilizando o Oracle Orion para comparar seus volumes, ele poderá simular a segmentação da mesma forma que o ASM do Oracle; portanto, recomendamos que você deixe a segmentação a cargo do Orion. Se você estiver usando uma ferramenta de comparação diferente, precisará fazer o stripe de volumes por conta própria.

Para obter instruções sobre como criar uma matriz RAID 0 com 6 volumes, consulte [Criar uma matriz RAID 0 no Linux \(p. 1469\)](#).

### 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. \(p. 1274\)](#). Para obter informações sobre como anexar esses volumes à sua instância, consulte [Vincular um volume de Amazon EBS a uma instância \(p. 1277\)](#).

A AWS fornece um modelo JSON para o uso com AWS CloudFormation que simplifica esse procedimento de configuração. Acesse o [modelo](#) e salve-o como um arquivo JSON. O AWS CloudFormation permite que

você configure suas próprias chaves SSH e oferece uma maneira mais fácil de configurar um ambiente de testes de performance para avaliar volumes `st1`. O modelo cria uma instância de geração atual e um volume `st1` de 2 TiB e anexa o volume à instância em `/dev/xvdf`.

#### Como criar um volume de HDD usando o modelo

1. Abra o console do AWS CloudFormation em <https://console.aws.amazon.com/cloudformation>.
2. Selecione Criar Stack.
3. Escolha Upload a Template to Amazon S3 e selecione o modelo JSON que você obteve anteriormente.
4. Dê um nome para a pilha como “ebs-perf- testes” e selecione um tipo de instância (o padrão é `r3.8xlarge`) e a chave SSH.
5. Selecione Next duas vezes e, em seguida, escolha Create Stack.
6. Depois que o status da nova pilha passar de CREATE\_IN\_PROGRESS para COMPLETE, escolha Outputs (Saídas) para obter a entrada de DNS público para sua nova instância, que terá um volume `st1` de 2 TiB anexado a ela.
7. Usando SSH, conecte-se à nova pilha como usuário `ec2-user`, com o nome de host obtido da entrada de DNS na etapa anterior.
8. Vá para [Instalar ferramentas de comparação \(p. 1474\)](#).

#### 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
<code>fio</code>	<p>Para comparar a performance de E/S. Observe que fio tem uma dependência sobre libaio-devel.</p> <p>Execute o comando a seguir para instalar o fio no Amazon Linux:</p> <pre>[ec2-user ~]\$ sudo yum install -y fio</pre> <p>Para instalar fio no Ubuntu, execute o seguinte comando:</p> <pre>sudo apt-get install -y fio</pre>
<code>Ferramenta de calibração do Oracle Orion</code>	Para calibrar a performance de E/S de sistemas de armazenamento a serem usados com bancos de dados do Oracle.

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 Linux

Você pode desativar os estados C no Amazon Linux, RHEL e CentOS da seguinte maneira:

1. Obtenha o número de estados C.

```
$ cpupower idle-info | grep "Number of idle states:"
```

2. Desative os estados C de c1 a cN. De preferência, os núcleos devem estar no estado c0.

```
$ for i in `seq 1 $((N-1))` ; do cpupower idle-set -d $i; done
```

## 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, inicialize-os antes do benchmarking. Para obter mais informações, consulte [Iniciar volumes de Amazon EBS \(p. 1466\)](#).

Quando você terminar de testar seus volumes, consulte os seguintes tópicos para obter ajuda para limpar: [Excluir um volume de Amazon EBS \(p. 1302\)](#) e [Encerrar a instância \(p. 587\)](#).

### Avalie a performance dos volumes de Provisioned IOPS SSD e Finalidade geral (SSD)

Execute fio na matriz RAID 0 que você criou.

O seguinte comando executa operações de gravação aleatórias de 16 KB.

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_volo --ioengine=psync --  
name=fio_test_file --direct=1 --rw=randwrite --bs=16k --size=1G --numjobs=16 --time_based  
--runtime=180 --group_reporting --norandommap
```

O seguinte comando executa operações de leitura aleatórias de 16 KB.

```
[ec2-user ~]$ sudo fio --directory=/mnt/p_iops_volo --name=fio_test_file --direct=1 --  
rw=randread --bs=16k --size=1G --numjobs=16 --time_based --runtime=180 --group_reporting --  
norandommap
```

Para obter mais informações sobre como interpretar os resultados, consulte este tutorial: [Inspeção de performance de E/S de disco com fio](#).

#### Avalie a performance dos volumes de st1 e sc1

Execute fio em seu volume do st1 ou sc1.

##### Note

Antes de executar esses testes, defina E/S em buffer na instância conforme descrito em [Aumentar a leitura antecipada para workloads com muita leitura e alta taxa de transferência em st1 e em sc1 \(p. 1462\)](#).

O seguinte comando executa operações de leitura sequenciais de 1 MiB em um dispositivo de blocos st1 anexado (por exemplo, /dev/xvdf):

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=read --randrepeat=0  
--ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --  
name=fio_direct_read_test
```

O seguinte comando executa operações de gravação sequenciais de 1 MiB em um dispositivo de blocos st1 anexado:

```
[ec2-user ~]$ sudo fio --filename=/dev/<device> --direct=1 --rw=write --randrepeat=0  
--ioengine=libaio --bs=1024k --iodepth=8 --time_based=1 --runtime=180 --  
name=fio_direct_write_test
```

Algumas workloads executam uma combinação de leituras e gravações sequenciais para diferentes partes de dispositivo de blocos. Para comparar essa workload, recomendamos que você use trabalhos de fio separados, simultâneos, para leituras e gravações, e use a opção fio offset\_increment para focar em locais diferentes de dispositivo de blocos para cada trabalho.

Executar essa workload é um pouco mais complicado do que uma workload de gravação ou leitura sequenciais. Use um editor de texto para criar um arquivo de trabalho de fio, chamado de fio\_rw\_mix.cfg neste exemplo, que contém o seguinte:

```
[global]  
clocksource=clock_gettime  
randrepeat=0  
runtime=180  
  
[sequential-write]  
bs=1M  
ioengine=libaio  
direct=1  
iodepth=8  
filename=/dev/<device>  
do_verify=0  
rw=write  
rwmixread=0
```

```
rwmixwrite=100  
  
[sequential-read]  
bs=1M  
ioengine=libaio  
direct=1  
iodepth=8  
filename=/dev/<device>  
do_verify=0  
rw=read  
rwmixread=100  
rwmixwrite=0  
offset=100g
```

Em seguida, execute o seguinte comando:

```
[ec2-user ~]$ sudo fio fio_rw_mix.cfg
```

Para obter mais informações sobre como interpretar os resultados, consulte este tutorial: [Inspeção de performance de E/S de disco com fio](#).

Vários trabalhos de fio para E/S direta, mesmo que usando operações de leitura ou gravação sequenciais, podem resultar em uma taxa de transferência mais baixa do que o esperado para volumes st1 e sc1. Recomendamos que você use um trabalho direto de E/S e use o parâmetro `iodepth` para controlar o número de operações simultâneas de E/S.

## 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 \(p. 1477\)](#)
- [Dimensões para métricas do Amazon EBS \(p. 1482\)](#)
- [Gráficos no console do Amazon EC2 \(p. 1482\)](#)

## 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 \(p. 1478\)](#)
- [Métricas de volume para volumes anexados a tipos de instância baseadas em Nitro \(p. 1482\)](#)

- [Métricas de restauração rápida do snapshot \(p. 1482\)](#)

## 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 \(p. 1288\)](#).

### 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 \(p. 210\)](#).
- 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 \(p. 880\)](#).

Métrica	Descrição
VolumeReadBytes	<p>Fornece informações sobre as operações de leitura 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 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 SampleCount 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 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>

Métrica	Descrição
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 <b>Minimum</b> e <b>Maximum</b> 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 <b>Minimum</b> e <b>Maximum</b> nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidades: contagem</p>
VolumeTotalReadTime	<p><b>Note</b></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 <b>Average</b> nessa métrica não é relevante para volumes anexados a instâncias baseadas em Nitro.</p> <p>As estatísticas <b>Minimum</b> e <b>Maximum</b> nessa métrica são compatíveis somente com volumes anexados às instâncias baseada em Nitro.</p> <p>Unidade: segundos</p>

Métrica	Descrição
<code>VolumeTotalWriteTime</code>	<p><b>Note</b></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>
<code>VolumeIdleTime</code>	<p><b>Note</b></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 <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>VolumeQueueLength</code>	<p>O número de solicitações de operação de leitura e gravação aguardando conclusão em um período de tempo especificado.</p> <p>A estatística <code>Sum</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>Unidades: contagem</p>

Métrica	Descrição
VolumeThroughputPercentage	<p><b>Note</b></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>
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 <a href="#">Créditos de E/S e performance de intermitência (p. 1257)</a>.</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 \(p. 880\)](#).

## Métricas de restauração rápida do snapshot

O namespace AWS/EBS inclui as métricas a seguir para [restauração rápida de snapshots \(p. 1430\)](#).

Métrica	Descrição
<code>FastSnapshotRestoreCreditsBucket</code>	O número máximo do volume cria créditos que podem ser acumulados. Essa métrica é informada por snapshot e por zona de disponibilidade.  A estatística mais significativa é Average. Os resultados das estatísticas de Minimum e Maximum são iguais aos de Average e podem ser usados no lugar.
<code>FastSnapshotRestoreCreditsBalance</code>	O número do volume cria créditos disponíveis. Essa métrica é informada por snapshot e por zona de disponibilidade.  A estatística mais significativa é Average. Os resultados das estatísticas de Minimum e Maximum são iguais aos de Average e podem ser usados no lugar.

## 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 \(p. 1478\)](#), 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 \(p. 1482\)](#), 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>

Gráfico	Descrição usando métricas brutas
Taxa de transferência de gravação (IOPS)	$\text{Sum}(\text{VolumeWriteOps}) / \text{Period}$
Comprimento médio da fila (operações)	$\text{Avg}(\text{VolumeQueueLength})$
% de tempo ocioso gasto	$\text{Sum}(\text{VolumeIdleTime}) / \text{Period} \times 100$
Tamanho médio de leitura (KiB/ operação)	<p><math>\text{Avg}(\text{VolumeReadBytes}) / 1024</math></p> <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera o tamanho médio de leitura usando a <a href="#">Matemática de métricas do CloudWatch</a>:</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>
Tamanho médio de gravação (KiB/ operação)	<p><math>\text{Avg}(\text{VolumeWriteBytes}) / 1024</math></p> <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera o tamanho médio de gravação usando a <a href="#">Matemática de métricas do CloudWatch</a>:</p> $(\text{Sum}(\text{VolumeWriteBytes}) / \text{Sum}(\text{VolumeWriteOps})) / 1024$ <p>As métricas <code>VolumeWriteBytes</code> e <code>VolumeWriteOps</code> estão disponíveis no console do EBS CloudWatch.</p>
Latência média de leitura (ms/ operação)	<p><math>\text{Avg}(\text{VolumeTotalReadTime}) \times 1000</math></p> <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera a latência média de leitura usando a <a href="#">Matemática de métricas do CloudWatch</a>:</p> $(\text{Sum}(\text{VolumeTotalReadTime}) / \text{Sum}(\text{VolumeReadOps})) \times 1000$ <p>As métricas <code>VolumeTotalReadTime</code> e <code>VolumeReadOps</code> estão disponíveis no console do EBS CloudWatch.</p>
Latência média de gravação (ms/ operação)	<p><math>\text{Avg}(\text{VolumeTotalWriteTime}) \times 1000</math></p> <p>Para as instâncias baseadas em Nitro, a fórmula a seguir gera a latência média de gravação usando a <a href="#">Matemática de métricas do CloudWatch</a>:</p> $(\text{Sum}(\text{VolumeTotalWriteTime}) / \text{Sum}(\text{VolumeWriteOps})) \times 1000$ <p>As métricas <code>VolumeTotalWriteTime</code> e <code>VolumeWriteOps</code> 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 \(p. 1484\)](#)
- [Eventos de snapshot do EBS \(p. 1487\)](#)
- [Eventos de modificação de volume do EBS \(p. 1491\)](#)
- [Eventos de restauração rápida do snapshot do EBS \(p. 1491\)](#)
- [Usar o AWS Lambda para lidar com o CloudWatch Events \(p. 1492\)](#)

## 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 \(createVolume\) \(p. 1484\)](#)
- [Excluir volume \(deleteVolume\) \(p. 1486\)](#)
- [Anexar ou reanexar volumes \(attachVolume, reattachVolume\) \(p. 1486\)](#)

### 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": "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",  
        "error": "KMS key is invalid or does not exist."  
    }  
}
```

```
"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 \(createSnapshot\) \(p. 1487\)](#)
- [Criar snapshots \(createSnapshots\) \(p. 1488\)](#)
- [Copiar snapshot \(copySnapshot\) \(p. 1489\)](#)
- [Compartilhar snapshot \(shareSnapshot\) \(p. 1490\)](#)

### 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 (createSchemas)

O evento `createSchemas` 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 `createSchemas` 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": "createSchemas",
        "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"  
            }  
        ]  
    }  
}
```

## 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": [  
        {  
            "snapshot_id": "arn:aws:ec2::us-east-1:snapshot/snap-012345678901"  
        }  
    ]  
}
```

```
    "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 share-snapshot. 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": "restored",  
        "start_time": "2015-06-10T12:00:00Z",  
        "end_time": "2015-06-10T12:05:00Z",  
        "status": "success",  
        "error": ""  
    }  
}
```

```
        "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 Habilitedo).
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).

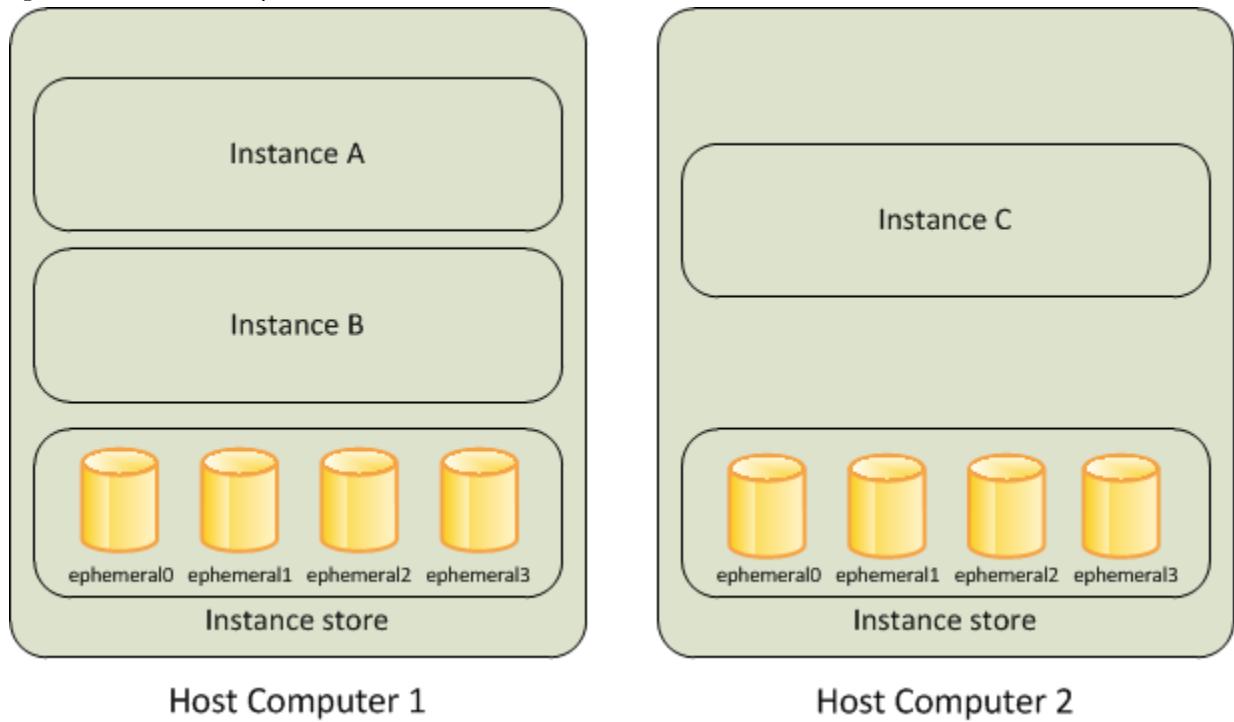
Para obter uma lista de cotas de serviço do Amazon EBS, consulte [Amazon Elastic Block Store endpoints and quotas](#) (Endpoints e cotas do Amazon Elastic Block Store) na AWS General Reference (Referência geral da AWS).

## 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 balanceamento 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 \(p. 1495\)](#)
- [Volumes de armazenamento de instâncias \(p. 1496\)](#)
- [Adicionar volumes de armazenamento de instâncias à instância do EC2 \(p. 1504\)](#)
- [Volumes de armazenamento de instâncias SSD \(p. 1508\)](#)
- [Volumes de troca de armazenamento de instâncias \(p. 1510\)](#)
- [Otimizar a performance dos discos para volumes de armazenamento de instâncias \(p. 1512\)](#)

## 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 acidentalmente), 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 \(p. 327\)](#).

## 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 \(p. 1504\)](#).

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 \(p. 1508\)](#).

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		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
c5ad.xlarge	1 x 150 GB	SSD de NVMe		✓
c5ad.2xlarge	1 x 300 GB	SSD de NVMe		✓
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		✓
c6gd.medium	1 x 59 GB	SSD de NVMe		✓
c6gd.large	1 x 118 GB	SSD de NVMe		✓
c6gd.xlarge	1 x 237 GB	SSD de NVMe		✓
c6gd.2xlarge	1 x 474 GB	SSD de NVMe		✓
c6gd.4xlarge	1 x 950 GB	SSD de NVMe		✓
c6gd.8xlarge	1 x 1.900 GB	SSD de NVMe		✓
c6gd.12xlarge	2 x 1.425 GB (2,85 TB)	SSD de NVMe		✓
c6gd.16xlarge	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
c6gd.metal	2 x 1.900 GB (3,8 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		

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Volumes de armazenamento de instâncias

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
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		
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		

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
<b>h1.4xlarge</b>	2 x 2.000 GB (4 TB)	HDD		
<b>h1.8xlarge</b>	4 x 2.000 GB (8 TB)	HDD		
<b>h1.16xlarge</b>	8 x 2.000 GB (16 TB)	HDD		
<b>hs1.8xlarge</b>	24 x 2.000 GB (48 TB)	HDD	✓	
<b>i2.xlarge</b>	1 x 800 GB	SSD		✓
<b>i2.2xlarge</b>	2 x 800 GB (1,6 TB)	SSD		✓
<b>i2.4xlarge</b>	4 x 800 GB (3,2 TB)	SSD		✓
<b>i2.8xlarge</b>	8 x 800 GB (6,4 TB)	SSD		✓
<b>i3.large</b>	1 x 475 GB	SSD de NVMe		✓
<b>i3.xlarge</b>	1 x 950 GB	SSD de NVMe		✓
<b>i3.2xlarge</b>	1 x 1.900 GB	SSD de NVMe		✓
<b>i3.4xlarge</b>	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
<b>i3.8xlarge</b>	4 x 1.900 GB (7,6 TB)	SSD de NVMe		✓
<b>i3.16xlarge</b>	8 x 1.900 GB (15,2 TB)	SSD de NVMe		✓
<b>i3.metal</b>	8 x 1.900 GB (15,2 TB)	SSD de NVMe		✓
<b>i3en.large</b>	1 x 1.250 GB	SSD de NVMe		✓
<b>i3en.xlarge</b>	1 x 2.500 GB	SSD de NVMe		✓
<b>i3en.2xlarge</b>	2 x 2.500 GB (5 TB)	SSD de NVMe		✓
<b>i3en.3xlarge</b>	1 x 7.500 GB	SSD de NVMe		✓
<b>i3en.6xlarge</b>	2 x 7.500 GB (15 TB)	SSD de NVMe		✓
<b>i3en.12xlarge</b>	4 x 7.500 GB (30 TB)	SSD de NVMe		✓
<b>i3en.24xlarge</b>	8 x 7.500 GB (60 TB)	SSD de NVMe		✓
<b>i3en.metal</b>	8 x 7.500 GB (60 TB)	SSD de NVMe		✓
<b>m1.small</b>	1 x 160 GB†	HDD	✓	
<b>m1.medium</b>	1 x 410 GB	HDD	✓	
<b>m1.large</b>	2 x 420 GB (840 GB)	HDD	✓	
<b>m1.xlarge</b>	4 x 420 GB (1,6 TB)	HDD	✓	
<b>m2.xlarge</b>	1 x 420 GB	HDD	✓	
<b>m2.2xlarge</b>	1 x 850 GB	HDD	✓	
<b>m2.4xlarge</b>	2 x 840 GB (1,68 TB)	HDD	✓	

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
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		✓
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		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
m6gd.medium	1 x 59 GB	SSD de NVMe		✓
m6gd.large	1 x 118 GB	SSD de NVMe		✓
m6gd.xlarge	1 x 237 GB	SSD de NVMe		✓
m6gd.2xlarge	1 x 474 GB	SSD de NVMe		✓
m6gd.4xlarge	1 x 950 GB	SSD de NVMe		✓
m6gd.8xlarge	1 x 1.900 GB	SSD de NVMe		✓
m6gd.12xlarge	2 x 1.425 GB (2,85 TB)	SSD de NVMe		✓
m6gd.16xlarge	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
m6gd.metal	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
p3dn.24xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
p4d.24xlarge	8 de 1.000 GB (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		✓
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		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
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		✓
r6gd.medium	1 x 59 GB	SSD de NVMe		✓
r6gd.large	1 x 118 GB	SSD de NVMe		✓
r6gd.xlarge	1 x 237 GB	SSD de NVMe		✓
r6gd.2xlarge	1 x 474 GB	SSD de NVMe		✓
r6gd.4xlarge	1 x 950 GB	SSD de NVMe		✓
r6gd.8xlarge	1 x 1.900 GB	SSD de NVMe		✓
r6gd.12xlarge	2 x 1.425 GB (2,85 TB)	SSD de NVMe		✓
r6gd.16xlarge	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
r6gd.metal	2 x 1.900 GB (3,8 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		
x2gd.medium	1 x 59 GB	SSD de NVMe		✓

Tipo de instância	Volumes de armazenamento de instâncias	Tipo	Precisa de inicialização*	Suporte para TRIM**
x2gd.large	1 x 118 GB	SSD de NVMe		✓
x2gd.xlarge	1 x 237 GB	SSD de NVMe		✓
x2gd.2xlarge	1 x 475 GB	SSD de NVMe		✓
x2gd.4xlarge	1 x 950 GB	SSD de NVMe		✓
x2gd.8xlarge	1 x 1.900 GB	SSD de NVMe		✓
x2gd.12xlarge	2 x 1.425 GB (2,85 TB)	SSD de NVMe		✓
x2gd.16xlarge	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
x2gd.metal	2 x 1.900 GB (3,8 TB)	SSD de NVMe		✓
z1d.large	1 x 75 GB	SSD de NVMe		✓
z1d.xlarge	1 x 150 GB	SSD de NVMe		✓
z1d.2xlarge	1 x 300 GB	SSD de NVMe		✓
z1d.3xlarge	1 x 450 GB	SSD de NVMe		✓
z1d.6xlarge	1 x 900 GB	SSD de NVMe		✓
z1d.12xlarge	2 x 900 GB (1,8 TB)	SSD de NVMe		✓
z1d.metal	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 [Otimizar a performance dos discos para volumes de armazenamento de instâncias \(p. 1512\)](#).

\*\* Para obter mais informações, consulte [Suporte a TRIM do volume de armazenamento de instâncias \(p. 1510\)](#).

† Os tipos de instância c1.medium e m1.small também incluem um volume de troca de armazenamento de instância de 900 MB que não pode ser automaticamente habilitado na hora da inicialização. Para obter mais informações, consulte [Volumes de troca de armazenamento de instâncias \(p. 1510\)](#).

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 \(p. 1530\)](#).

Um mapeamento de dispositivos de blocos sempre especifica o volume raiz da instância. O volume raiz é um volume do Amazon EBS ou um volume do armazenamento de instâncias. Para obter mais informações, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#). O volume raiz é montado automaticamente. Para instâncias com um volume de armazenamento de instâncias do volume de raiz, o tamanho desse volume varia por AMI, mas o tamanho máximo é 10 GB.

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 \(p. 1250\)](#).

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 \(p. 327\)](#).

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 \(p. 1496\)](#).

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 \(p. 1505\)](#)
- [Adicionar volumes de armazenamento de instâncias a uma instância \(p. 1506\)](#)
- [Disponibilizar volumes de armazenamento de instâncias na instância \(p. 1507\)](#)

## 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 disponível para a instância, os volumes de armazenamento de instâncias adicionais serão ignorados.

#### Considerações

- 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 armazenamento 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 significativa 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 Linux. \(p. 1528\)](#).) 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 Linux. \(p. 1528\)](#).) 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, execute o comando `lsblk`.

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 \(p. 1510\)](#). 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 \(p. 1539\)](#).

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 do Windows](#).

Em instâncias Linux, você pode visualizar e montar os volumes de armazenamento de instâncias conforme descrito no procedimento a seguir.

Para disponibilizar um volume de armazenamento de instâncias no Linux

1. Conecte-se à instância usando um cliente SSH. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. Use o comando `df -h` para visualizar os volumes formatados e montados.

```
[ec2-user ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/devtmpfs        3.8G   72K  3.8G   1% /dev
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Use o `lsblk` para visualizar todos os volumes que foram mapeados na inicialização, mas não formatados e montados.

```
[ec2-user ~]$ lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1    259:1    0   8G  0 disk
##nvme0n1p1 259:2    0   8G  0 part /
##nvme0n1p128 259:3   0   1M  0 part
nvme1n1    259:0    0 69.9G 0 disk
```

4. Para formatar e montar um volume de armazenamento de instâncias que foi apenas mapeado, faça o seguinte:

- a. Crie um sistema de arquivos no dispositivo usando o comando `mkfs`.

```
[ec2-user ~]$ sudo mkfs -t xfs /dev/nvme1n1
```

- b. Crie um diretório no qual montar o dispositivo usando o comando `mkdir`.

```
[ec2-user ~]$ sudo mkdir /data
```

- c. Monte o dispositivo no diretório recém-criado usando o comando `mount`.

```
[ec2-user ~]$ sudo mount /dev/nvme1n1 /data
```

Para obter instruções sobre como montar um volume associado automaticamente após a reinicialização, consulte [Montar automaticamente um volume anexado após a reinicialização \(p. 1285\)](#).

## Volumes de armazenamento de instâncias SSD

Para garantir a melhor performance de IOPS nos volumes de armazenamento de instâncias SSD no Linux, recomendamos usar uma versão mais recente do Amazon Linux ou outra AMI do Linux com uma versão de kernel de 3.8 ou superior. Se você não usar a AMI do Linux com uma versão de kernel de 3.8 ou superior, sua instância não atingirá a performance máxima de IOPS disponível para esses tipos de instância.

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 \(p. 1504\)](#).

## 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 \(p. 1496\)](#).

Para acessar os volumes de NVMe, os [drivers de NVMe \(p. 1434\)](#) devem ser instalados. As AMIs a seguir atendem a este requisito:

- Amazon Linux 2
- Amazon Linux AMI 2018.03
- Ubuntu 14.04 (com kernel `linux-aws`) ou posterior
- Red Hat Enterprise Linux 7.4 ou posterior
- SUSE Linux Enterprise Server 12 SP2 ou posterior
- CentOS 7.4.1708 ou posterior
- FreeBSD 11.1 ou posterior
- Debian GNU/Linux 9 ou posterior

Depois de se conectar à instância, você pode listar os dispositivos de NVMe usando o comando `lspci`. O seguinte é um exemplo da saída de uma instância `i3.8xlarge` compatível com quatro dispositivos de NVMe.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Se você está usando um sistema operacional compatível mas os dispositivos de NVMe não estão sendo exibidos, verifique se o módulo de NVMe está carregado usando o comando a seguir.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

```
$ lsmod | grep nvme
nvme           48813  0
```

- Ubuntu 18

```
$ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
s/nvme/host/nvme-core.ko
kernel/drivers/nvme/host/nvme.ko
kernel/drivers/nvmmem/nvmmem_core.ko
```

Os volumes de NVMe estão em conformidade com a especificação NVMe 1.0e. Você pode usar os comandos de NVMe com os volumes de NVMe. Com o Amazon Linux, você pode instalar o pacote `nvme-cli` no repositório usando o comando `yum install`. Com outras versões compatíveis do Linux, você pode fazer download do pacote `nvme-cli` se ele não estiver disponível na imagem.

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 \(p. 1496\)](#).

## 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 \(p. 1496\)](#).

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.

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 Linux, use o comando `fstrim` para habilitar o TRIM periódico.

## Volumes de troca de armazenamento de instâncias

O espaço de troca no Linux pode ser usado quando um sistema precisa de mais memória que a que foi alocada fisicamente. Quando o espaço de troca está habilitado, os sistemas Linux podem mudar páginas da memória física usadas infrequentemente para espaço de troca (uma partição dedicada ou um arquivo de troca em um sistema de arquivos existente) e liberar esse espaço para páginas de memória que exigem acesso de alta velocidade.

### Note

O uso do espaço de troca para paginação de memória não é tão rápido ou eficiente quanto usar a RAM. Se a workload estiver paginando a memória regularmente no espaço de troca, você deve considerar migrar para um tipo de instância maior com mais memória RAM. Para obter mais informações, consulte [Alterar o tipo de instância \(p. 327\)](#).

Os tipos de instância `c1.medium` e `m1.small` têm uma quantidade limitada de memória física para trabalhar e recebem um volume de troca de 900 MiB no momento do lançamento para atuar como memória virtual para AMIs do Linux. Embora o kernel do Linux veja esse espaço de troca como uma partição no dispositivo raiz, ele é na verdade um volume separado para armazenamento de instâncias, independentemente do tipo de dispositivo raiz.

O Amazon Linux habilita e usa automaticamente esse espaço de troca, mas a AMI pode exigir algumas etapas adicionais para reconhecer e usar esse espaço de troca. Para ver se a instância está usando o espaço de troca, você pode usar o comando `swapon -s`.

```
[ec2-user ~]$ swapon -s
Filename                Type      Size    Used   Priority
/dev/xvda3              partition 917500  0       -1
```

A instância acima tem um volume de troca de 900 MiB anexado e habilitado. Se você não vir um volume de troca listado com esse comando, você poderá precisar habilitar o espaço de troca para o dispositivo. Verifique os discos disponíveis usando o comando lsblk.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0   8G  0 disk /
xvda3 202:3    0  896M 0 disk
```

Aqui, o volume de troca xvda3 está disponível para a instância, mas não está habilitado (observe que o campo MOUNTPOINT está vazio). Você pode habilitar o volume de troca com o comando swapon.

#### Note

Você precisa preceder /dev/ ao nome do dispositivo listado pelo lsblk. Seu dispositivo pode ter um nome diferente, como sda3, sde3 ou xvde3. Use o nome do dispositivo de seu sistema no comando abaixo.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

Agora o espaço de troca deve ser mostrado na saída do lsblk e do swapon -s.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0   8G  0 disk /
xvda3 202:3    0  896M 0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename            Type      Size  Used  Priority
/dev/xvda3          partition 917500  0     -1
```

Também será necessário editar o arquivo /etc/fstab para que esse espaço de troca seja habilitado automaticamente em cada inicialização do sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Acrescente a linha a seguir ao arquivo /etc/fstab (usando o nome do dispositivo de troca de seu sistema):

```
/dev/xvda3 none swap sw 0 0
```

Para usar um volume de armazenamento de instâncias como espaço de troca

Qualquer volume de armazenamento de instâncias pode ser usado como espaço de troca. Por exemplo, o tipo de instância m3.medium inclui um volume de armazenamento de instâncias SSD de 4 GB que é adequado para o espaço de troca. Se o volume de armazenamento de instâncias for muito maior (por exemplo, 350 GB), você poderá considerar particionar o volume com uma partição de troca menor de 4 a 8 GB e o restante para um volume de dados.

#### Note

Esse procedimento se aplica apenas a tipos de instância que oferecem suporte ao armazenamento de instâncias. Para obter uma lista dos tipos de instâncias compatíveis, consulte [Volumes de armazenamento de instâncias \(p. 1496\)](#).

1. Liste os dispositivos de blocos anexados à instância para obter o nome do dispositivo de seu volume de armazenamento de instâncias.

```
[ec2-user ~]$ lsblk -p
```

```
NAME      MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
/dev/xvda1 202:1    0   8G  0 disk /
```

Neste exemplo, o volume de armazenamento de instâncias é `/dev/xvdb`. Como essa é uma instância do Amazon Linux, o volume de armazenamento de instâncias está formatado e montado em `/media/ephemeral0`. Nem todos os sistemas operacionais Linux fazem isso automaticamente.

2. (Opcional) Se o volume de armazenamento de instâncias está montado (ele é listado como um `MOUNTPOINT` na saída do comando `lsblk`), você precisa desmontá-lo com o comando a seguir.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Configure uma área de troca do Linux no dispositivo com o comando `mkswap`.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Habilite o novo espaço de troca.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Verifique se o novo espaço de troca está sendo usado.

```
[ec2-user ~]$ swapon -s
Filename      Type  Size Used Priority
/dev/xvdb          partition 4188668 0 -1
```

6. Edite o arquivo `/etc/fstab` para que esse espaço de troca seja habilitado automaticamente em cada inicialização do sistema.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Se o arquivo `/etc/fstab` tiver uma entrada para `/dev/xvdb` (ou para `/dev/sdb`) altere-o para que corresponda à linha abaixo. Se ele não tiver uma entrada para esse dispositivo, adicione a linha a seguir no arquivo `/etc/fstab` (usando o nome do dispositivo de troca de seu sistema):

```
/dev/xvdb      none      swap      sw  0      0
```

#### Important

Os dados do volume de armazenamento de instâncias são perdidos quando uma instância é interrompida ou hibernada. Isso inclui a formatação do espaço de troca do armazenamento de instâncias criadas em [Step 3 \(p. 1512\)](#). Se você parar e reiniciar uma instância que foi configurada para usar o espaço de troca de armazenamento de instâncias, deverá repetir a [Step 1 \(p. 1511\)](#) até a [Step 5 \(p. 1512\)](#) no novo volume de armazenamento de instâncias.

## Otimizar a performance dos discos para volumes de armazenamento de instâncias

Por causa do modo como o Amazon EC2 virtualiza os discos, a primeira gravação em qualquer local em alguns volumes de armazenamento de instâncias ocorre mais lentamente que as gravações subsequentes. Para a maioria das aplicações, a amortização desse custo ao longo da vida útil da instância

é aceitável. Entretanto, se você precisar de alta performance de disco, recomendamos inicializar suas unidades gravando uma vez em todos os locais da unidade antes do uso em produção.

Note

Alguns tipos de instância com discos de estado sólido (SSD) anexados diretamente e suporte a TRIM fornecem performance máxima no momento da inicialização, sem inicialização. Para obter informações sobre o armazenamento de instâncias para cada tipo de instância, consulte [Volumes de armazenamento de instâncias \(p. 1496\)](#).

Se você precisar de maior flexibilidade na latência ou no throughput, recomendamos usar o Amazon EBS.

Para inicializar os volumes de armazenamento de instâncias, use os seguintes comandos dd, dependendo do armazenamento a ser inicializado (por exemplo, /dev/sdb ou /dev/nvme1n1).

Note

Desmonte a unidade antes de executar esse comando.

A inicialização pode levar muito tempo (cerca de oito horas para uma instância extragrande).

Para inicializar os volumes de armazenamento de instâncias, use os comandos a seguir nos tipos de instância m1.large, m1.xlarge, c1.xlarge, m2.xlarge, m2.2xlarge e m2.4xlarge:

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Para executar a inicialização em todos os volumes de armazenamento de instâncias ao mesmo tempo, use o comando a seguir:

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

A configuração de unidades para RAID as inicializa gravando em todos os locais da unidade. Ao configurar o RAID com base em software, altere a velocidade mínima da reconstrução:

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

## 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 Linux.

Tópicos

- [Usar o Amazon S3 com a Amazon EC2 \(p. 1514\)](#)

- [Usar o Amazon EFS com o Amazon EC2 \(p. 1515\)](#)

## 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 \(p. 1248\)](#).

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.

GET ou wget

O utilitário wget é um cliente FTP e HTTP que permite a você fazer download de objetos públicos no Amazon S3. Por padrão, ele é armazenado no Linux da Amazon e na maioria de outras distribuições e está disponível para download no Windows. Para fazer download de um objeto do Amazon S3, use o comando a seguir substituindo a URL do objeto para download.

```
[ec2-user ~]$ wget https://my_bucket.s3.amazonaws.com/path-to-file
```

O método exige que o objeto solicitado seja público. Se o objeto não for público, você receberá uma mensagem de "ERROR 403: Forbidden". Se você receber esse erro, abra o console do Amazon S3 e altere as permissões do objeto para públicas. Para obter mais informações, consulte o [Amazon Simple Storage Service Developer Guide](#) (Guia do desenvolvedor do Amazon Simple Storage Service).

#### 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.

```
[ec2-user ~]$ 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.

```
[ec2-user ~]$ 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.

```
[ec2-user ~]$ 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.

Você pode montar um sistema de arquivos do EFS na sua instância das seguintes maneiras:

#### Tópicos

- [Criar um sistema de arquivos do EFS usando a Criação rápida do Amazon EFS \(p. 1516\)](#)
- [Criar um sistema de arquivos de EFS e montá-lo na sua instância \(p. 1517\)](#)

## Criar um sistema de arquivos do EFS usando a Criação rápida do Amazon EFS

Você pode criar um sistema de arquivos do EFS e montá-lo na sua instância no momento da inicialização usando o recurso Criação rápida do Amazon EFS do Launch Wizard de instâncias.

Quando você cria um sistema de arquivos do EFS usando a Criação rápida do EFS, o sistema de arquivos é criado com as seguintes configurações recomendadas de serviço:

- Backups automáticos ativados. Para obter mais informações, consulte [Using AWS Backup with Amazon EFS](#) (Usar o AWS Backup com o Amazon EFS) no Amazon Elastic File System User Guide (Manual do usuário do Amazon Elastic File System).
- Monte destinos em cada sub-rede padrão na VPC selecionada, usando o grupo de segurança padrão da VPC. Para obter mais informações, consulte [Gerenciar a acessibilidade da rede do sistema de arquivos](#) no Manual do usuário do Amazon Elastic File System.
- Modo de performance de uso geral Para obter mais informações, consulte [Modos de performance](#) no Manual do usuário do Amazon Elastic File System.
- Modo de taxa de transferência intermitente. Para obter mais informações, consulte [Modos de taxa de transferência](#) no Manual do usuário do Amazon Elastic File System.
- Criptografia de dados em repouso habilitada usando a chave padrão para o Amazon EFS (`aws / elasticfilesystem`). Para obter mais informações, consulte [Criptografia de dados em repouso](#) no Manual do usuário do Amazon Elastic File System.
- Gerenciamento do ciclo de vida do Amazon EFS habilitado com uma política de 30 dias. Para obter mais informações, consulte [Gerenciamento de ciclo de vida](#) do EFS no Manual do usuário do Amazon Elastic File System.

Para criar um sistema de arquivos do EFS usando a Criação Rápida do Amazon EFS

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 AMI (Escolher uma), escolha uma AMI do Linux.
4. Na página Choose an Instance Type (Escolher um tipo de instância), selecione um tipo de instância e escolha Next: Configure Instance Details (Avançar: configurar os detalhes da instância).
5. Na página Configure Instance Details (Configurar detalhes da instância), em File systems (Sistemas de arquivos), escolha Create new file system (Criar novo sistema de arquivos), insira um nome para o novo sistema de arquivos e escolha Create (Criar).

Para habilitar o acesso ao sistema de arquivos, os grupos de segurança a seguir são automaticamente criados e anexados à instância e aos destinos de montagem do sistema de arquivos.

- O Grupo de segurança da instância—não inclui regras de entrada e uma regra de saída que permitem o tráfego pela porta NFS 2049.
- O Grupo de segurança de destinos de montagem do sistema de arquivos—Inclui uma regra de entrada que permite o tráfego pela porta NFS 2049 proveniente do grupo de segurança da instância (descrito acima) e uma regra de saída que permite o tráfego pela porta NFS 2049.

Você também pode optar por criar e anexar manualmente os grupos de segurança. Para fazer isso, desmarque Criar e anexar automaticamente os grupos de segurança necessários.

Configure as definições remanescentes conforme necessário e escolha Next: Add Storage (Avançar: Adicionar armazenamento).

6. Na página Add Storage (Adicionar armazenamento), especifique os volumes para anexar às instâncias, além dos volumes especificados pela AMI (como o volume do dispositivo raiz). Certifique-se de provisionar armazenamento suficiente para o toolkit Nvidia CUDA. Depois, selecione Next: Add Tags (Próximo: adicionar tags).
7. Na página Add Tags (Adicionar tags), especifique uma tag que você pode usar para identificar a instância temporária e escolha Next: Configure Security Group (Próximo: configurar grupo de segurança).
8. Na página Configure Security Group (Configurar grupo de segurança), revise os grupos de segurança e escolha Review and Launch (Revisar e executar).
9. Na página Review Instance Launch (Revisar execução da instância), reveja as configurações e escolha Launch (Executar) para escolher um par de chaves e executar a instância.

## Criar um sistema de arquivos de EFS e montá-lo na sua instância

Neste tutorial, você cria um sistema de arquivos de EFS e duas instâncias Linux que podem compartilhar dados usando o sistema de arquivos.

### Tarefas

- [Prerequisites \(p. 1517\)](#)
- [Etapa 1: criar um sistema de arquivos do EFS \(p. 1517\)](#)
- [Etapa 2: montar o sistema de arquivos \(p. 1518\)](#)
- [Etapa 3: testar o sistema de arquivos \(p. 1519\)](#)
- [Etapa 4: Limpeza \(p. 1519\)](#)

### Prerequisites

- Crie um security group (por exemplo, efs-sg) a ser associado às instâncias do EC2 e ao destino de montagem do EFS, além de adicionar as seguintes regras:
  - Permita conexões SSH de entrada às instâncias do EC2 no computador (a origem é o bloco CIDR da rede).
  - Permita conexões NFS de entrada com o sistema de arquivos pelo destino de montagem do EFS nas instâncias do EC2 associadas a esse security group (a origem é o próprio security group). Para obter mais informações, consulte [Regras do Amazon EFS \(p. 1244\)](#) e [Criar grupos de segurança](#) no Guia do usuário do Amazon Elastic File System.
- Criar um par de chaves. Você deve especificar um par de chaves ao configurar suas instâncias ou não será possível se conectar a elas. Para obter mais informações, consulte [Criar um par de chaves \(p. 5\)](#).

### Etapa 1: criar um sistema de arquivos do EFS

O Amazon EFS permite criar um sistema de arquivos que várias instâncias podem montar e acessar ao mesmo tempo. Para obter mais informações, consulte [Criação de recursos do Amazon EFS](#) no Guia do usuário do Amazon Elastic File System.

Para criar um sistema de arquivos

1. Abra o console do Amazon Elastic File System em <https://console.aws.amazon.com/efs/>.
2. Escolha Create file system (Criar sistema de arquivos).
3. (Opcional) Em Name (Nome), insira um nome para o sistema de arquivos. Isso cria uma tag com Nome como a chave e o nome do sistema de arquivos como o valor.

4. Em Virtual Private Cloud (VPC), selecione a VPC a ser usada para suas instâncias.
5. Escolha Create (Criar).
6. Depois que o sistema de arquivos for criado, observe o ID do sistema de arquivos. Ele será usado mais tarde neste tutorial.
7. Escolha o ID do sistema de arquivos.
8. Na página de sistemas de arquivos, escolha Network (Rede), Manage (Gerenciar). Exiba os destinos de montagem criados pelo Amazon EFS em cada zona de disponibilidade na região em que sua VPC reside. Para cada zona de disponibilidade das suas instâncias, certifique-se de que o valor de Security groups (Grupos de segurança) seja o grupo de segurança criado em [Prerequisites \(p. 1517\)](#).
9. Escolha Save (Salvar).

## Etapa 2: montar o sistema de arquivos

Use o procedimento a seguir para executar duas instâncias `t2.micro`. Observe que as instâncias T2 devem ser executadas em uma sub-rede. Você pode usar uma VPC padrão ou uma VPC não padrão.

### Note

Há outras formas de você montar o volume (por exemplo, em uma instância já em execução). Para obter mais informações, consulte [Montagem de sistemas de arquivos](#) no Guia do usuário do Amazon Elastic File System.

Para executar duas instâncias e montar um sistema de arquivos de EFS

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 do Amazon Linux.
4. Em Step 2: Choose an Instance Type (Etapa 2: escolher um tipo de instância), mantenha o tipo de instância padrão, `t2.micro`, e selecione Next: Configure Instance Details (Próximo: Configurar detalhes da instância).
5. Na Etapa 3: Configurar os detalhes da instância, faça o seguinte:
  - a. Em Number of instances (Número de instâncias), insira **2**.
  - b. [VPC padrão] Se você tiver uma VPC padrão, é o valor padrão para Network (Rede). Mantenha a VPC e o valor padrão para Subnet (Sub-rede) para usar a sub-rede padrão na zona de disponibilidade que o Amazon EC2 escolher para suas instâncias.  
[VPC não padrão] Selecione sua VPC para Network (Rede) e uma sub-rede pública em Subnet (Sub-rede).
  - c. [VPC não padrão] Em Auto-assign Public IP (Atribuir IP público automaticamente), selecione Enable (Habilitar). Caso contrário, suas instâncias não terão endereços IP públicos nem nomes DNS públicos.
  - d. Em File systems (Sistemas de arquivos), escolha Add file system (Adicionar sistema de arquivos). Verifique se o valor corresponde ao ID do sistema de arquivos que você criou em [Etapa 1: criar um sistema de arquivos do EFS \(p. 1517\)](#). O caminho mostrado ao lado do ID do sistema de arquivos é o ponto de montagem que a instância usará, que pode ser alterado. Em Advanced Details (Detalhes avançados), os User data (Dados do usuário) são gerados automaticamente e incluem os comandos necessários para montar o sistema de arquivos.
  - e. Avance para a etapa 6 do assistente.
6. Na página Configure Security Group (Configurar grupo de segurança), selecione Select an existing security group (Selecionar um grupo de segurança existente) e selecione o grupo de segurança que você criou em [Prerequisites \(p. 1517\)](#). Depois, selecione Review and Launch (Verificar e ativar).
7. Na página Review Instance Launch, escolha Launch.

8. 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), selecione Choose an existing key pair (Escolher um par de chaves existente) e escolha seu par de chaves. Selecione a caixa de seleção de confirmação e escolha Launch Instances (Executar instâncias).
9. No painel de navegação, escolha Instances (Instâncias) para visualizar o status de suas instâncias. Inicialmente, seu status é pending. Depois que o status mudar para running, suas instâncias estarão prontas para uso.

Agora a instância está configurada para montar o sistema de arquivos do Amazon EFS na execução e sempre que for reinicializada.

### Etapa 3: testar o sistema de arquivos

Você pode se conectar às suas instâncias e verificar se o sistema de arquivos está montado no diretório especificado (por exemplo, /mnt/efs).

Para verificar se o sistema de arquivos está montado

1. Conecte-se às instâncias. Para obter mais informações, consulte [Conecte-se à sua instância do Linux \(p. 535\)](#).
2. Na janela do terminal de cada instância, execute o comando df -T para verificar se o sistema de arquivos EFS está montado.

```
$ df -T
Filesystem      Type            1K-blocks   Used       Available Use% Mounted on
/dev/xvda1      ext4           8123812  1949800        6073764  25% /
devtmpfs        devtmpfs        4078468     56        4078412  1% /dev
tmpfs           tmpfs           4089312     0        4089312  0% /dev/shm
efs-dns         nfs4          9007199254740992     0        9007199254740992  0% /mnt/efs
```

O nome do sistema de arquivos, mostrado na saída do exemplo como **efs-dns**, tem a seguinte forma.

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. (Opcional) Crie um arquivo no sistema de arquivos com base em uma instância e verifique se é possível visualizar o arquivo pela outra instância.
  - a. Na primeira instância, execute o seguinte comando para criar o arquivo.

```
$ sudo touch /mnt/efs/test-file.txt
```

- b. Na segunda instância, execute o seguinte comando para visualizar o arquivo.

```
$ ls /mnt/efs
test-file.txt
```

### Etapa 4: Limpeza

Ao concluir este tutorial, você pode encerrar as instâncias e excluir o sistema de arquivos.

Para encerrar as instâncias

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, escolha Instances (Instâncias).

3. Selecione as instâncias para encerrar.
4. Escolha Instance state (Estado da instância) e Terminate instance (Encerrar instância).
5. Quando a confirmação for solicitada, escolha Terminate (Encerrar).

Para excluir o sistema de arquivos

1. Abra o console do Amazon Elastic File System em <https://console.aws.amazon.com/efs/>.
2. Selecione o sistema de arquivos a ser excluído.
3. Escolha Actions (Ações), Delete file system (Excluir sistema de arquivos).
4. Quando a confirmação for solicitada, insira o ID do sistema de arquivos e escolha Delete file system (Excluir sistema de arquivos).

## 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 \(p. 1520\)](#)
- [Limites de volumes específicos do Linux \(p. 1521\)](#)
- [Largura de banda x capacidade \(p. 1521\)](#)

## Limites de volumes do Sistema Nitro

As instâncias criadas no [Sistema Nitro \(p. 210\)](#) 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 \(p. 984\)](#) e [Volumes de armazenamento de instâncias \(p. 1496\)](#).

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.
- As instâncias inf1.xlarge e inf1.2xlarge oferecem suporte a um máximo de 26 volumes do EBS.
- inf1.6xlarge As instâncias oferecem suporte a um máximo de 23 volumes do EBS.
- inf1.24xlarge As instâncias oferecem suporte a um máximo de 11 volumes do EBS.
- A maioria das instâncias bare metal oferece suporte a um máximo de 31 volumes do EBS.
- mac1.metal As instâncias oferecem suporte a um máximo de 16 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 Linux

Anexar mais de 40 volumes pode causar falhas de inicialização. Esse número inclui o volume raiz, mais os volumes do EBS e os volumes de armazenamento de instâncias anexados. Se você tiver problemas de inicialização em uma instância com um grande número de volumes, interrompa a instância, desanexe todos os volumes que não são essenciais ao processo de inicialização e anexe novamente os volumes depois que a instância estiver em execução.

**Important**

Anexar mais de 40 volumes a uma instância Linux tem suporte somente em uma base de melhor esforço e não é garantido.

## 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 \(p. 1438\)](#) 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 lançamos o Amazon EC2, todas as AMIs tinham armazenamento de instâncias do Amazon EC2, o que significa que o dispositivo raiz de uma instância executada a partir da AMI é um volume de armazenamento de instâncias criado com base em um modelo armazenado no Amazon S3. Depois que lançamos o Amazon EBS, apresentamos as AMIs com Amazon EBS. Isso significa que o dispositivo raiz de uma instância executada na AMI é um volume do Amazon EBS criado de um snapshot do Amazon EBS.

Você pode escolher entre as AMIs com armazenamento de instâncias do Amazon EC2 e as AMIs com Amazon EBS. Recomendamos que você use AMIs com Amazon EBS, pois elas são executadas mais rapidamente e usam armazenamento persistente.

**Important**

Somente os seguintes tipos de instância oferecem suporte a um volume de armazenamento de instâncias como o dispositivo raiz: C3, D2, G2, I2, M3 e R3.

Para obter mais informações sobre os nomes de dispositivos usados pelo Amazon EC2 para seus volumes raiz, consulte [Nomes de dispositivos em instâncias do Linux. \(p. 1528\)](#).

### Tópicos

- [Conceitos de armazenamento do dispositivo raiz \(p. 1522\)](#)
- [Escolher uma AMI por tipo de dispositivo raiz \(p. 1523\)](#)
- [Determinar o tipo de dispositivo raiz da instância \(p. 1524\)](#)

- Alterar o volume raiz para persistir (p. 1525)
- Alterar o tamanho inicial do volume raiz (p. 1528)

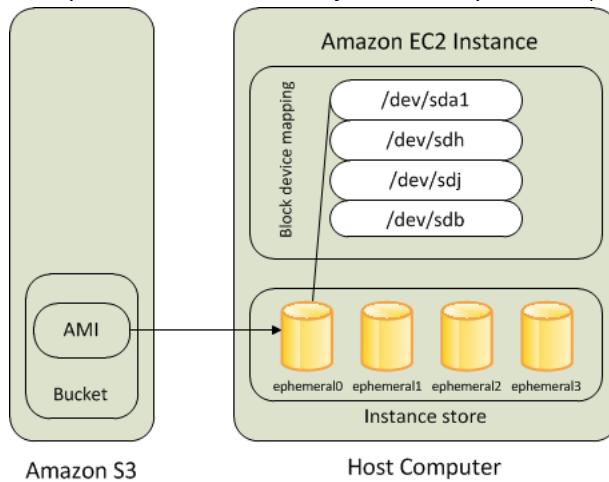
## Conceitos de armazenamento do dispositivo raiz

Você pode executar uma instância da AMI com armazenamento de instâncias ou da AMI com Amazon EBS. A definição de uma AMI inclui que tipo de AMI ela é. Você encontrará referências ao dispositivo raiz em alguns lugares como ebs (com Amazon EBS) ou como `instance store` (com armazenamento de instâncias). Isso é importante, pois há diferenças significativas entre o que você pode fazer com cada tipo de AMI. Para obter mais informações sobre essas diferenças, consulte [Armazenamento para o dispositivo raiz \(p. 75\)](#).

### Instâncias baseadas em armazenamento de instâncias

As instâncias que usam armazenamentos de instâncias para o dispositivo raiz automaticamente têm um ou mais volumes de armazenamento de instâncias disponíveis, com volume servindo como volume de dispositivo raiz. Quando uma instância é executada, a imagem usada para inicializá-la é copiada para o volume do dispositivo raiz. Observe que você também usar volumes adicionais de armazenamento de instâncias, dependendo do tipo de instância.

Todos os dados nos volumes de armazenamento de instâncias são mantidos desde que a instância esteja em execução, mas esses dados serão excluídos quando a instância for encerrada (instâncias com armazenamento de instâncias não oferecem suporte à ação Stop (Interromper)) ou se ela falhar (por exemplo, se uma unidade subjacente tiver problemas).

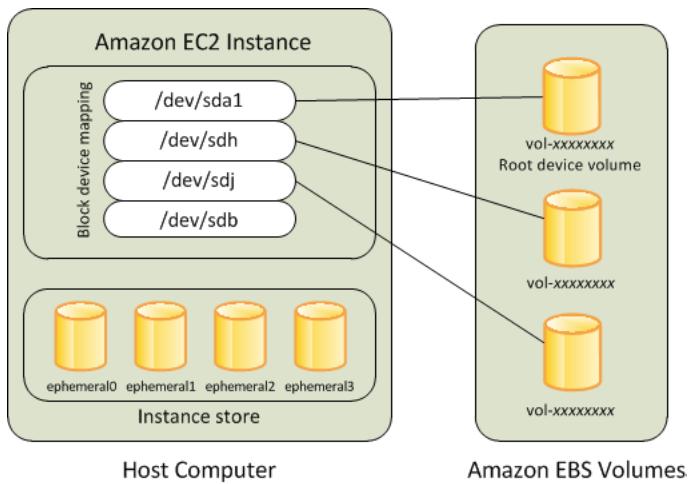


Após uma instância com armazenamento de instâncias falhar ou ser encerrada, ela não poderá ser restaurada. Se você planeja usar as instâncias baseadas em armazenamento de instâncias no Amazon EC2, recomendamos enfaticamente que distribua os dados nos seus armazenamentos de instâncias através de várias zonas de disponibilidade. Você também deve fazer backup dos dados críticos dos volumes de armazenamento de instâncias para o armazenamento persistente regularmente.

Para obter mais informações, consulte [Armazenamento de instâncias do Amazon EC2 \(p. 1494\)](#).

### Instâncias com Amazon EBS

As instâncias que usam o Amazon EBS para dispositivo raiz automaticamente têm um volume do Amazon EBS associado. Quando você executa uma instância com Amazon EBS, criamos um volume do Amazon EBS para cada snapshot do Amazon EBS mencionado pela AMI que você usa. Você também pode usar outros volumes do Amazon EBS ou volumes de armazenamento de instâncias, dependendo do tipo de instância.



Uma instância com Amazon EBS pode ser interrompida e posteriormente reiniciada sem afetar os dados armazenados nos volumes associados. Há várias tarefas relacionadas a instâncias e volumes que você pode realizar quando uma instância com Amazon EBS estiver em estado interrompido. Por exemplo, você pode modificar as propriedades da instância, alterar seu tamanho ou atualizar o kernel que está usando ou você pode associar o volume de raiz a uma instância em execução diferente para depuração ou qualquer outra finalidade.

Se uma instância com Amazon EBS falhar, você poderá restaurar sua sessão seguindo um dos seguintes métodos:

- Pare e reinicie (teste esse método primeiro).
- Faça automaticamente o snapshot de todos os volumes relevantes e crie uma nova AMI. Para obter mais informações, consulte [Criar uma AMI do Linux baseada em Amazon EBS \(p. 107\)](#).
- Associe o volume à nova instância seguindo estas etapas:
  1. Crie um snapshot de novo volume raiz.
  2. Registre a nova AMI usando o snapshot.
  3. Execute uma nova instância a partir da nova AMI.
  4. Separe os volumes do Amazon EBS restantes da instância antiga.
  5. Reassocie os volumes do Amazon EBS à nova instância.

Para obter mais informações, consulte [Volumes do Amazon EBS \(p. 1250\)](#).

## Escolher uma AMI por tipo de dispositivo raiz

A AMI que você especifica ao executar a instância determina o tipo de volume de dispositivo raiz que sua instância tem. Você pode visualizar AMIs por tipo de dispositivo raiz usando um dos métodos a seguir.

### Console

Para selecionar uma AMI com Amazon EBS usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, selecione AMIs.
3. Nas listas de filtros, selecione o tipo de imagem (por exemplo, Public images (Imagens públicas)). Na barra de pesquisa, escolha Platform (Plataforma) para selecionar o sistema operacional (como Amazon Linux) e Root Device Type (Tipo de dispositivo raiz) para selecionar EBS images (Imagens EBS).

4. (Opcional) Para obter informações adicionais para ajudá-lo a fazer sua escolha, selecione o ícone Show/Hide Columns (Mostrar/ocultar colunas), atualize as colunas a serem exibidas e escolha Close (Fechar).
5. Escolha uma AMI e anote seu ID da AMI.

Para selecionar uma AMI com armazenamento de instâncias usando o console

1. Abra o console do Amazon EC2.
2. No painel de navegação, selecione AMIs.
3. Nas listas de filtros, selecione o tipo de imagem (por exemplo, Public images (Imagens públicas)). Na barra de pesquisa, escolha Platform (Plataforma) para selecionar o sistema operacional (como Amazon Linux) e Root Device Type (Tipo de dispositivo raiz) para selecionar Instance store (Armazenamento de instâncias).
4. (Opcional) Para obter informações adicionais para ajudá-lo a fazer sua escolha, selecione o ícone Show/Hide Columns (Mostrar/ocultar colunas), atualize as colunas a serem exibidas e escolha Close (Fechar).
5. Escolha uma AMI e anote seu ID da AMI.

#### AWS CLI

Para verificar o tipo de volume do dispositivo raiz de 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 \(p. 3\)](#).

- [describe-images \(AWS CLI\)](#)
- [Get-EC2Image \(AWS Tools for Windows PowerShell\)](#)

## Determinar o tipo de dispositivo raiz da instância

### New console

Para determinar o tipo de dispositivo raiz 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 a instância.
3. Na guia Storage (Armazenamento), em Root device details (Detalhes do dispositivo raiz), verifique o valor de Root device type (Tipo de dispositivo raiz), da seguinte maneira:
  - Se o valor for EBS, essa será uma instância com Amazon EBS.
  - Se o valor for INSTANCE-STORE, essa será uma instância com armazenamento de instâncias.

### Old console

Para determinar o tipo de dispositivo raiz 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 a instância.
3. Na guia Description (Descrição), verifique o valor de Root device type (Tipo de dispositivo raiz) da seguinte maneira:
  - Se o valor for ebs, essa será uma instância com Amazon EBS.

- Se o valor for `instance store`, essa será uma instância com armazenamento de instâncias.

#### AWS CLI

Para determinar o tipo de dispositivo raiz 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)

## Alterar o volume raiz para persistir

Por padrão, o volume raiz de uma AMI com Amazon EBS é excluído quando a instância é encerrada. Você pode alterar o comportamento padrão para garantir que o volume persista após a interrupção da instância. Para alterar o comportamento padrão, defina o atributo `DeleteOnTermination` como `false` usando um mapeamento de dispositivos de blocos.

#### Tarefas

- [Configurar o volume raiz para persistir durante a execução da instância \(p. 1525\)](#)
- [Configurar o volume raiz para persistir em uma instância existente \(p. 1526\)](#)
- [Confirmar que um volume raiz está configurado para persistir \(p. 1527\)](#)

## 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`.

```
$ 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`.

```
$ 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-
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 \(p. 1535\)](#).
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 \(p. 1318\)](#).
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 \(p. 1536\)](#), 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 do dispositivos de blocos da AMI.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
        "VolumeSize": 100
    }
}
```

Para obter mais informações, consulte [Mapeamentos de dispositivos de blocos \(p. 1530\)](#).

## Nomes de dispositivos em instâncias do Linux.

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 \(p. 1520\)](#).

#### Tópicos

- [Nomes de dispositivos disponíveis \(p. 1529\)](#)
- [Considerações sobre nomes de dispositivos \(p. 1530\)](#)

Para obter informações sobre os nomes de dispositivos em instâncias do Windows, consulte [Nomenclatura de dispositivos em instâncias do Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## Nomes de dispositivos disponíveis

Há dois tipos de virtualização disponíveis para instâncias do Linux: paravirtual (PV) e máquina virtual de hardware (HVM). O tipo de virtualização de uma instância é determinado pela AMI usada para executar a instância. Todos os tipos de instância são compatíveis com AMIs HVM. Alguns tipos de instância da geração anterior oferecem suporte a AMIs PV. Observe o tipo de virtualização da AMI, pois os nomes de dispositivos recomendados e disponíveis que você pode usar dependem do tipo de virtualização da instância. Para obter mais informações, consulte [Tipos de virtualização da AMI em Linux \(p. 77\)](#).

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 virtualização	Disponível	Reservado para raiz	Recomendado para volumes do EBS	Volumes de armazenamento de instâncias
Paravirtual	/dev/sd[a-z]  /dev/sd[a-z][1-15]  /dev/hd[a-z]  /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p]  /dev/sd[f-p][1-6]	/dev/sd[b-e]
HVM	/dev/sd[a-z]  /dev/xvd[b-c][a-z]	Difere por AMI  /dev/sda1 ou /dev/xvda	/dev/sd[f-p] *  /dev/sd [] BH (h1.16xlarge)  /dev/sd[b-y] (d2.8xlarge)  /dev/sd[b-i] (i2.8xlarge)	/dev/sd[b-e]  /dev/sd [] BH (h1.16xlarge)  /dev/sd[b-y] (d2.8xlarge)  /dev/sd[b-i] (i2.8xlarge)  **

\* Os nomes de dispositivo que você especifica para volumes NVMe do EBS no mapeamento de dispositivos de blocos são renomeados usando nomes de dispositivo de NVMe (/dev/nvme[0-26]n1). O driver do dispositivo de blocos pode atribuir nomes de dispositivos NVMe em uma ordem diferente da especificada para os volumes no mapeamento de dispositivos de blocos.

\*\* Os volumes de armazenamento de instâncias NVMe são automaticamente enumerados e atribuídos a um nome de dispositivo NVMe.

Para obter mais informações sobre volumes de armazenamento de instâncias, consulte [Armazenamento de instâncias do Amazon EC2 \(p. 1494\)](#). 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 Linux \(p. 1434\)](#).

## 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 um nome de dispositivo NVMe (`/dev/nvme[0-26]n1`).
- Dependendo do driver do dispositivo de bloco do kernel, o dispositivo pode ser anexado com um nome diferente do especificado por você. Por exemplo, se você especificar um nome de dispositivo de `/dev/sdh`, o dispositivo poderá ser renomeado como `/dev/xvdh` ou `/dev/hdh`. Na maioria dos casos, a letra à direita permanece a mesma. Em algumas versões do Red Hat Enterprise Linux (e suas variantes, como o CentOS), a letra à direita pode ser alterada (`/dev/sda` pode se tornar `/dev/xvde`). Nesses casos, a letra à direita de cada nome de dispositivo é aumentada no mesmo número de vezes. Por exemplo, se `/dev/sdb` é renomeado `/dev/xvdf`, então `/dev/sdc` é renomeado `/dev/xvdg`. O Amazon Linux cria um link simbólico para o nome que você especificou no dispositivo renomeado. Outros sistemas operacionais podem se comportar de maneira diferente.
- As AMIs HVM não oferecem suporte ao uso de números à esquerda nos nomes de dispositivo, exceto `/dev/sda1`, que é reservado para o dispositivo raiz, e `/dev/sda2`. Embora o uso de `/dev/sda2` seja possível, não recomendamos o uso desse mapeamento de dispositivo com instâncias HVM.
- Ao usar AMIs PV, você não pode anexar volumes que compartilham as mesmas letras de dispositivos com e sem dígitos à direita. Por exemplo, se você anexar um volume como `/dev/sdc` e outro volume como `/dev/sdc1`, somente `/dev/sdc` será visível para a instância. Para usar dígitos à direita em nomes de dispositivos, você deve usar dígitos à direita em todos os nomes de dispositivos que compartilham as mesmas letras base (como `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- Alguns kernels personalizados podem ter restrições que limitam o uso a `/dev/sd[f-p]` ou `/dev/sd[f-p][1-6]`. Se estiver tendo problema para usar `/dev/sd[q-z]` ou `/dev/sd[q-z][1-6]`, tente mudar para `/dev/sd[f-p]` ou `/dev/sd[f-p][1-6]`.

## 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 \(p. 1277\)](#). 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 [Alterar o volume raiz para persistir \(p. 1525\)](#).

### Tópicos

- [Conceitos de mapeamento de dispositivos de blocos \(p. 1531\)](#)
- [Mapeamento de dispositivos de blocos da AMI \(p. 1534\)](#)
- [Mapeamento de dispositivos de blocos de instância \(p. 1536\)](#)

## 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 \(p. 1531\)](#)
- [Advertências do armazenamento de instâncias de mapeamento de dispositivos de blocos \(p. 1532\)](#)
- [Exemplo de mapeamento de dispositivos de blocos \(p. 1533\)](#)
- [Como os dispositivos são disponibilizados no sistema operacional \(p. 1533\)](#)

## 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 Linux. \(p. 1528\)](#).

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.

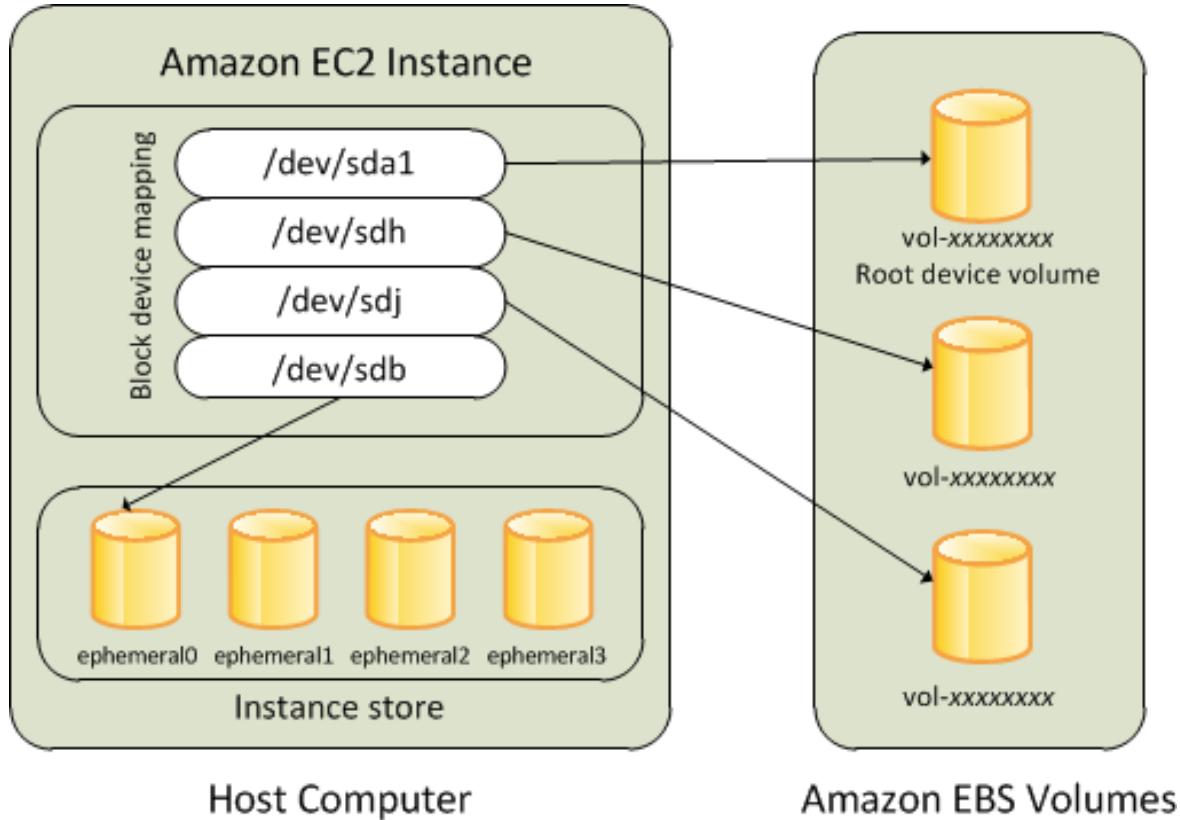
### Note

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 \(p. 1534\)](#) e [Atualizar o mapeamento de dispositivos de blocos ao executar uma instância \(p. 1536\)](#).

## 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 Linux, os nomes de dispositivo especificados no mapeamento de dispositivos de blocos serão mapeados para os dispositivos de blocos quando a instância for inicializada pela primeira vez. O tipo de instância determina quais volumes de armazenamento de instâncias são formatados e montados por padrão. Você pode montar volumes de armazenamento de instâncias adicionais na execução, desde que não ultrapasse o número de volumes de armazenamento de instâncias disponível.

para seu tipo de instância. Para obter mais informações, consulte [Armazenamento de instâncias do Amazon EC2 \(p. 1494\)](#). O driver do dispositivo de blocos para a instância determina quais dispositivos são usados quando os volumes são formatados e montados. Para obter mais informações, consulte [Vincular um volume de Amazon EBS a uma instância \(p. 1277\)](#).

## 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 \(p. 1534\)](#)
- [Visualizar os volumes do EBS em um mapeamento de dispositivo de blocos da AMI \(p. 1535\)](#)

## 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 AMI 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": "/dev/sdf",  
    "VirtualName": "ephemeral0"  
}
```

Para adicionar um volume vazio do gp2 de 100 GiB, use o mapeamento a seguir.

```
{  
    "DeviceName": "/dev/sdg",  
    "Ebs": {  
        "VolumeSize": 100  
    }  
}
```

Para adicionar um volume do EBS com base em um snapshot, use o mapeamento a seguir.

```
{  
    "DeviceName": "/dev/sdh",  
    "Ebs": {  
        "SnapshotId": "snap-xxxxxxxx"  
    }  
}
```

Para omitir um mapeamento de um dispositivo, use o mapeamento a seguir:

```
{  
    "DeviceName": "/dev/sdj",  
    "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 \(p. 1536\)](#)
- [Atualizar o mapeamento de dispositivos de blocos de uma instância em execução \(p. 1538\)](#)
- [Visualizar os volumes do EBS em um mapeamento de dispositivos de blocos de instância \(p. 1538\)](#)
- [Visualizar o mapeamento de dispositivos de blocos de instância para volumes de armazenamento de instâncias \(p. 1539\)](#)

## 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:

- `/dev/sdb=ephemeral0`
- `/dev/sdh=snap-1234567890abcdef0`
- `/dev/sdj=:100`

Para evitar que o `/dev/sdj` seja anexado a uma instância em execução nesta AMI, use o mapeamento a seguir.

```
{  
    "DeviceName": "/dev/sdj",  
    "NoDevice": ""  
}
```

Para aumentar o tamanho de `/dev/sdh` para 300 GiB, especifique o mapeamento a seguir. Observe que você não precisa especificar o ID do snapshot para `/dev/sdh`, pois especificar o nome do dispositivo basta para identificar o volume.

```
{  
    "DeviceName": "/dev/sdh",  
    "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, /dev/sdc, 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": "/dev/sdc",  
    "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 AWS não 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, /dev/sdf e /dev/sdj)

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 \(p. 1287\)](#).

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 \(p. 649\)](#).

Primeiro, conecte-se à instância em execução. Com base na instância, use esta consulta para obter o mapeamento de dispositivos de blocos.

#### 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/
```

#### IMDSv1

```
[ec2-user ~]$ curl 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
```

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 para a instância, execute o comando `lsblk`. Para saber a quantidade de volumes de armazenamento de instâncias compatível com cada tipo de instância, consulte [Volumes de armazenamento de instâncias \(p. 1496\)](#).

# 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 \(p. 1542\)](#)
- [IDs de recursos \(p. 1543\)](#)
- [Listar e filtrar seus recursos \(p. 1544\)](#)
- [Marcar com tag os recursos do Amazon EC2 \(p. 1552\)](#)
- [Cotas de serviço do Amazon EC2 \(p. 1565\)](#)
- [Relatórios de uso do Amazon EC2 \(p. 1567\)](#)

## 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 <a href="#">Copiar um AMI (p. 144)</a> .
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 <a href="#">Copiar um snapshot do Amazon EBS. (p. 1313)</a> .
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 <a href="#">Pares de chaves do Amazon EC2 e instâncias do Linux (p. 1209)</a> .
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 \(p. 1545\)](#)
- [Listar e filtrar usando a CLI e a API \(p. 1549\)](#)

- [Listar e filtrar recursos entre Regiões usando o Amazon EC2 Global View \(p. 1551\)](#)

## Listar e filtrar recursos usando o console

### Sumário

- [Listar recursos usando o console \(p. 1545\)](#)
- [Filtrar recursos usando o console \(p. 1545\)](#)

### 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 \(p. 1561\)](#).

## 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

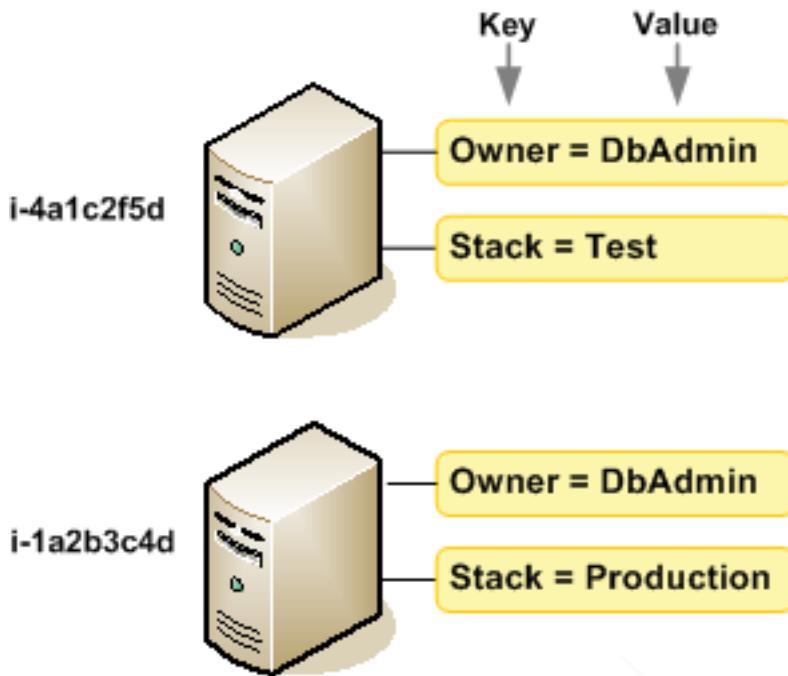
- [Conceitos básicos de tags \(p. 1552\)](#)
- [Marcar com tag os recursos do \(p. 1553\)](#)
- [Restrições de tags \(p. 1556\)](#)
- [Gerenciamento de tags e acesso \(p. 1557\)](#)
- [Marcar com tag recursos para faturamento \(p. 1557\)](#)
- [Trabalhar com tags usando o console \(p. 1558\)](#)
- [Trabalhar com tags usando a linha de comando \(p. 1561\)](#)
- [Adicionar tags a um recurso usando o CloudFormation \(p. 1564\)](#)

## 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 \(p. 1554\)](#) 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 \(p. 1144\)](#).

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 \(p. 1554\)](#).

## 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 \(p. 1144\)](#).

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 \(p. 1544\)](#).

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 \(p. 1558\)](#)
- [Adicionar e excluir tags em um recurso individual \(p. 1559\)](#)
- [Adicionar e excluir tags a um grupo de recursos \(p. 1560\)](#)
- [Adicionar uma tag ao executar uma instância \(p. 1560\)](#)
- [Filtrar uma lista de recursos por tag \(p. 1561\)](#)

## 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 de 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 \(p. 1542\)](#).
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 \(p. 1542\)](#).
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 \(p. 1542\)](#).
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 \(p. 1542\)](#).
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 \(p. 1542\)](#).
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 Linux \(p. 87\)](#).
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 \(p. 1544\)](#).

## 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	<a href="#">create-tags</a>	<a href="#">New-EC2Tag</a>
Exclua uma ou mais tags	<a href="#">delete-tags</a>	<a href="#">Remove-EC2Tag</a>
Descreva uma ou mais tags	<a href="#">describe-tags</a>	<a href="#">Get-EC2Tag</a>

### Tarefas

- [Adicionar tags na criação de recursos \(p. 1561\)](#)
- [Adicionar tags a um recurso existente \(p. 1562\)](#)
- [Descrever recursos marcados com tags \(p. 1563\)](#)

## 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.

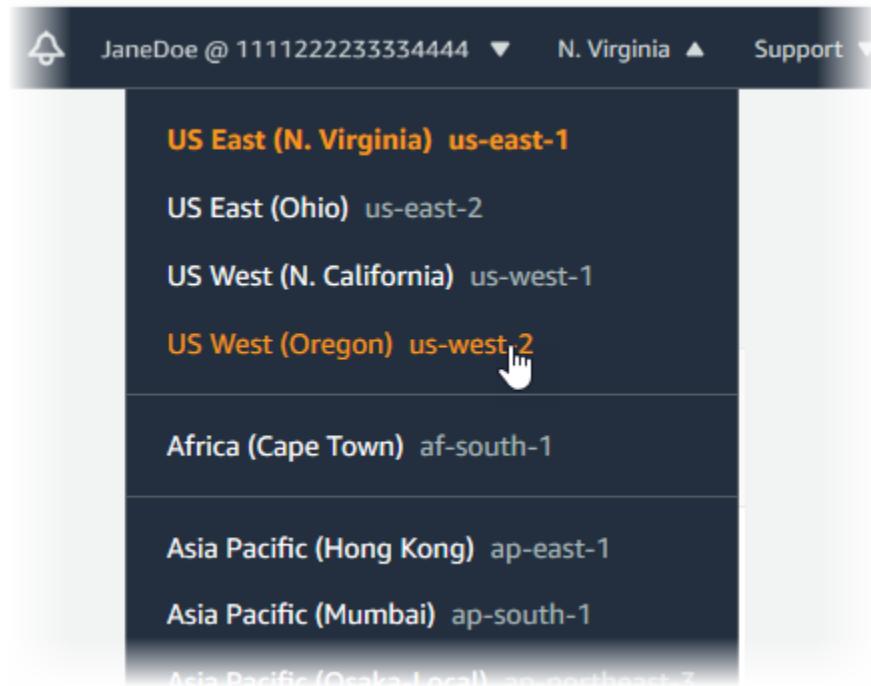
Para obter mais informações, consulte [Endpoints e cotas do Amazon EC2](#) na Referência geral do Amazon Web Services. Para obter informações sobre cotas do Amazon EBS, consulte [Cotas do Amazon EBS \(p. 1494\)](#).

## 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 do EC2

A documentação a seguir podem ajudar a solucionar problemas que você venha a ter com sua instância.

## Tópicos

- [Solucionar problemas de execução de instâncias \(p. 1568\)](#)
- [Solução de problemas para conectar-se à sua instância \(p. 1571\)](#)
- [Solução de problemas na interrupção da instância \(p. 1583\)](#)
- [Solucionar problemas de encerramento \(desativação\) da instância \(p. 1585\)](#)
- [Solução de problemas em instâncias com falha nas verificações de status \(p. 1586\)](#)
- [Solucionar problemas de uma instância não acessível \(p. 1609\)](#)
- [Inicialização a partir do volume errado \(p. 1612\)](#)
- [Usar o EC2Rescue para Linux \(p. 1613\)](#)
- [EC2 Serial Console para instâncias do Linux \(p. 1623\)](#)
- [Enviar uma interrupção para diagnóstico \(para usuários avançados\) \(p. 1640\)](#)

Para obter mais ajuda com instâncias do Windows, consulte [Solução de problemas de instâncias Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## Solucionar problemas de execução de instâncias

Os problemas a seguir impedem que você execute uma instância.

### Problemas de execução

- [Limite de instâncias excedido \(p. 1568\)](#)
- [Capacidade insuficiente da instância \(p. 1569\)](#)
- [A configuração solicitada não é suportada atualmente. Verifique a documentação quanto às configurações compatíveis. \(p. 1569\)](#)
- [A instância é encerrada imediatamente \(p. 1570\)](#)

## 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 \(p. 1565\)](#).

# 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 \(p. 327\)](#).
- 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 \(p. 1087\)](#).

**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 \(p. 326\)](#).

# 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 \(p. 1520\)](#).
- 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).

# Solução de problemas para conectar-se à sua instância

As informações a seguir podem ajudar você a solucionar problemas de conexão com a instância. Para obter mais ajuda com instâncias do Windows, consulte [Solução de problemas de instâncias Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

### Problemas e erros de conexão

- [Causas comuns de problemas de conexão \(p. 1571\)](#)
- [Erro ao se conectar à sua instância: limite de tempo da conexão atingido \(p. 1572\)](#)
- [Erro: não foi possível carregar a chave ... Esperando: QUALQUER CHAVE PRIVADA \(p. 1576\)](#)
- [Erro: Chave do usuário não reconhecida pelo servidor \(p. 1576\)](#)
- [Erro: permissão negada ou conexão fechada pela porta 22 de \[instância\] \(p. 1577\)](#)
- [Erro: arquivo de chave privada desprotegido \(p. 1579\)](#)
- [Erro: a chave privada deve começar com "----BEGIN RSA PRIVATE KEY----" e terminar com "----END RSA PRIVATE KEY----" \(p. 1580\)](#)
- [Erro: o servidor recusou nossa chave ou não há métodos de autenticação compatíveis disponíveis \(p. 1580\)](#)
- [Não é possível fazer o ping da instância \(p. 1581\)](#)
- [Erro: Server unexpectedly closed network connection \(A conexão de rede foi fechada inesperadamente pelo servidor\) \(p. 1581\)](#)
- [Erro: falha na validação da chave do host para EC2 Instance Connect \(p. 1581\)](#)

## Causas comuns de problemas de conexão

Recomendamos que você comece a solucionar problemas verificando algumas causas comuns para problemas de conexão com a instância.

### Verificar o nome de usuário da instância

É possível se conectar à instância usando o nome de usuário da conta de usuário ou o nome de usuário padrão da AMI usada para executar a instância.

- Obtenha o nome de usuário da sua conta de usuário.

Para obter mais informações sobre como criar uma conta de usuário, consulte [Gerenciar contas de usuário na instância do Amazon Linux \(p. 602\)](#).

- Obtenha o nome de usuário padrão da AMI usada para executar a instância:

- Para o Amazon Linux 2 ou a AMI do Amazon Linux, o nome do usuário é `ec2-user`.
- Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
- Para uma AMI do Ubuntu, o nome do usuário é `admin`.
- Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
- Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
- Para uma AMI do Bitnami, o nome do usuário é `bitnami`.
- Caso contrário, verifique com o provedor da AMI.

Verificar se as regras do grupo de segurança permitem tráfego

Verificar se as regras do grupo de segurança permitem o tráfego de entrada do endereço IPv4 público na porta adequada. Para obter as etapas de verificação, consulte [Erro ao se conectar à sua instância: limite de tempo da conexão atingido \(p. 1572\)](#)

Verificar se a instância está pronta

Depois de iniciar uma instância, pode demorar alguns minutos para ela ficar pronta e que você possa se conectar a ela. Verifique a instância para se certificar de que ela está sendo executada e passou em suas verificações de status.

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. Verifique o seguinte:
  - a. Na coluna Instance state (Estado da instância), verifique se sua instância está no estado `running`.
  - b. Na coluna Status check (Verificação de status), verifique se sua instância passou nas duas verificações de status.

Verifique os pré-requisitos gerais para se conectar à instância

Para obter mais informações, consulte [Pré-requisitos gerais para conectar-se à instância \(p. 535\)](#).

## Erro ao se conectar à sua instância: limite de tempo da conexão atingido

Se você tentar se conectar à sua instância e receber uma mensagem de erro `Network error: Connection timed out` ou `Error connecting to [instance], reason: -> Connection timed out: connect`, experimente o seguinte:

Verifique as regras do seu security group.

Você precisa de uma regra do security group que permita tráfego de entrada a partir do seu endereço IPv4 público na porta apropriada.

#### New 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 Security (Segurança) na parte inferior da página do console, em Inbound rules (Regras de entrada), verifique a lista de regras que estão em vigor para a instância selecionada.
  - Para instâncias do Linux: verifique se há uma regra para permitir tráfego do seu computador para a porta 22 (SSH).
  - Para instâncias do Windows: verifique se há uma regra para permitir tráfego do seu computador para a porta 3389 (RDP).
4. Cada vez que sua instância for reiniciada, um novo endereço IP (e nome de host) será atribuído. Se o grupo de segurança tiver uma regra que permite tráfego de entrada de um único endereço IP, esse endereço não poderá ser estático caso seu computador esteja em uma rede corporativa ou caso você esteja se conectando por um provedor de serviços de Internet (ISP). Em vez disso, especifique o intervalo de endereços IP usado por computadores do cliente. Se seu security group não tiver uma regra que permita tráfego de entrada como descrito na etapa anterior, adicione uma regra para seu security group. Para obter mais informações, consulte [Autorizar tráfego de entrada para suas instâncias do Linux \(p. 1205\)](#).

Para obter mais informações sobre regras de grupos de segurança, consulte [Regras de grupos de segurança](#) no Guia do usuário da Amazon VPC.

#### Old 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 Description (Descrição) na parte inferior da página do console, ao lado de Security groups (Grupos de segurança), selecione view inbound rules (visualizar regras de entrada) para exibir a lista de regras que estão em vigor para a instância selecionada.
4. Para instâncias do Linux: quando você selecionar view inbound rules (visualizar regras de entrada), será exibida uma janela que exibe a(s) porta(s) para a(s) qual(is) o tráfego é permitido. Verifique se há uma regra para permitir tráfego de seu computador para a porta 22 (SSH).

Para instâncias do Windows: quando você selecionar view inbound rules (visualizar regras de entrada), será exibida uma janela que exibe a(s) porta(s) para a(s) qual(is) o tráfego é permitido. Verifique se há uma regra para permitir tráfego de seu computador para a porta 3389 (RDP).

Cada vez que sua instância for reiniciada, um novo endereço IP (e nome de host) será atribuído. Se o security group tiver uma regra que permite tráfego de entrada de um único endereço IP, esse endereço não poderá ser estático se seu computador estiver em uma rede corporativa ou se você estiver se conectando por um provedor de Internet (ISP). Em vez disso, especifique o intervalo de endereços IP usado por computadores do cliente. Se seu security group não tiver uma regra que permita tráfego de entrada como descrito na etapa anterior, adicione uma regra para seu security group. Para obter mais informações, consulte [Autorizar tráfego de entrada para suas instâncias do Linux \(p. 1205\)](#).

Para obter mais informações sobre regras de grupos de segurança, consulte [Regras de grupos de segurança](#) no Guia do usuário da Amazon VPC.

Verifique a tabela de rotas para a sub-rede.

Você precisa de uma rota que envie todo o tráfego que sai da VPC para o gateway da Internet da VPC.

#### New 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 Networking (Redes), anote os valores para VPC ID (ID da VPC) e Subnet ID (ID de sub-rede).
4. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
5. No painel de navegação, escolha Gateways da Internet. Verifique se há um gateway de internet associado à sua VPC. Caso contrário, escolha Create internet gateway (Criar gateway da Internet), insira um nome para o gateway da Internet e escolha Create internet gateway (Criar gateway da Internet). Em seguida, para o gateway da internet criado, escolha Actions (Ações), Attach to VPC (Anexar à VPC), selecione sua VPC e, em seguida, escolha Attach internet gateway (Anexar gateway da internet) para anexá-lo à sua VPC.
6. No painel de navegação, selecione Sub-redes e selecione sua sub-rede.
7. Na guia Route tabl (Tabela de rotas), verifique se há uma rota com 0.0.0.0/0 como destino e o gateway da Internet para sua VPC como alvo. Se você estiver se conectando à sua instância usando o endereço IPv6, verifique que há uma rota para todo o tráfego IPv6 (:/:0) que aponta para o gateway de Internet. Caso contrário, faça o seguinte:
  - a. Escolha o ID da tabela de rotas (rtb-xxxxxxxx) para navegar para a tabela de rotas.
  - b. Na guia Routes (Rotas), escolha Edit routes (Editar rotas). Escolha Add route (Adicionar rota), use 0.0.0.0/0 como o destino, e o gateway da Internet como o destino. Para IPv6, escolha Add route (Adicionar rota), use ::/0 como o destino, e o gateway da Internet como o destino.
  - c. Escolha Save routes (Salvar rotas).

#### Old 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 Descrição, anote os valores de ID de VPC e ID da sub-rede.
4. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
5. No painel de navegação, escolha Gateways da Internet. Verifique se há um gateway de internet associado à sua VPC. Caso contrário, escolha Criar gateway da internet para criar um gateway da Internet. Selecione o gateway de internet e escolha Associar à VPC e siga as instruções para associá-la à sua VPC.
6. No painel de navegação, selecione Sub-redes e selecione sua sub-rede.
7. Na guia Tabela de rotas, verifique que há uma rota com 0.0.0.0/0 como o destino e o gateway de Internet para sua VPC como destino. Se você estiver se conectando à sua instância usando o endereço IPv6, verifique que há uma rota para todo o tráfego IPv6 (:/:0) que aponta para o gateway de Internet. Caso contrário, faça o seguinte:
  - a. Escolha o ID da tabela de rotas (rtb-xxxxxxxx) para navegar para a tabela de rotas.
  - b. Na guia Routes (Rotas), escolha Edit routes (Editar rotas). Escolha Add route (Adicionar rota), use 0.0.0.0/0 como o destino, e o gateway da Internet como o destino. Para IPv6, escolha Add route (Adicionar rota), use ::/0 como o destino, e o gateway da Internet como o destino.
  - c. Escolha Save routes (Salvar rotas).

Verifique a lista de controle de acesso (ACL) da rede para a sub-rede.

As ACLs da rede devem permitir tráfego de entrada do seu endereço IP local na porta 22 (para instâncias do Linux) ou na porta 3389 (para instâncias do Windows). Também deve permitir tráfego de saída para as portas efêmeras (1024-65535).

1. Abra o console da Amazon VPC em <https://console.aws.amazon.com/vpc/>.
2. No painel de navegação, escolha Sub-redes.
3. Selecione a sub-rede.
4. Na guia Network ACL (ACL da rede), em Inbound rules,(Regras de entrada), verifique se as regras permitem tráfego de entrada na porta obrigatória de seu computador. Caso contrário, exclua ou modifique a regra que está bloqueando tráfego.
5. Em Outbound rules (Regras de saída), verifique se as regras permitem tráfego nas portas efêmeras para seu computador. Caso contrário, exclua ou modifique a regra que está bloqueando tráfego.

Caso seu computador esteja em uma rede corporativa

Pergunte ao administrador da rede se o firewall interno permite tráfego de entrada e saída do seu computador na porta 22 (para instâncias do Linux) ou na porta 3389 (para instâncias do Windows).

Se você tiver um firewall no seu computador, verifique se ele permite tráfego de entrada e de saída do seu computador na porta 22 (para instâncias do Linux) ou na porta 3389 (para instâncias do Windows).

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 \(p. 975\)](#).

Verifique a carga de CPU na sua instância; o servidor pode estar sobrecarregado.

A AWS fornece automaticamente dados, como status de métricas e instâncias de Amazon CloudWatch, que você pode usar para ver quanta carga de CPU está na sua instância e, caso necessário, ajusta como suas cargas são manuseadas. Para obter mais informações, consulte [Monitorar instâncias usando o CloudWatch \(p. 872\)](#).

- Se sua carga for variável, você poderá expandir ou reduzir automaticamente suas instâncias usando o [Auto Scaling](#) e o [Elastic Load Balancing](#).
- Se sua carga estiver crescendo constantemente, é possível mudá-la para um tipo de instância maior. Para obter mais informações, consulte [Alterar o tipo de instância \(p. 327\)](#).

Para conectar-se à sua instância usando um endereço IPv6, verifique o seguinte:

- Sua sub-rede deve estar associada a uma tabela de rotas que tenha uma rota para tráfego IPv6 (: : /0) para um gateway de Internet.
- As regras do security group devem permitir tráfego de entrada do seu endereço IPv6 local na porta apropriada (22 para Linux e 3389 para Windows).
- As regras de Network ACL devem permitir tráfego de IPv6 de entrada e saída.
- Se você executou a instância de uma AMI mais antiga, ela pode não estar configurada para DHCPv6 (endereços IPv6 não são automaticamente reconhecidos na interface de rede). Para obter mais informações, consulte [Configurar o IPv6 em suas instâncias](#) no Guia do usuário da Amazon VPC.
- Seu computador local deve ter um endereço IPv6 e ser configurado para usar IPv6.

## Erro: não foi possível carregar a chave ... Esperando: QUALQUER CHAVE PRIVADA

Se você tentar se conectar à sua instância e obter a mensagem de erro `unable to load key ...`, o arquivo no qual a chave privada está armazenada foi configurado incorretamente. Se o arquivo da chave privada terminar em `.pem`, ele ainda poderá estar configurado incorretamente. Uma possível causa para um arquivo da chave privada configurado incorretamente é a ausência de um certificado.

Se o arquivo da chave privada estiver configurado incorretamente, siga estas etapas para solucionar o erro:

1. Crie um novo par de chaves. Para obter mais informações, consulte [Criar um par de chaves usando o Amazon EC2 \(p. 1210\)](#).
2. Adicione o novo par de chaves à sua instância. Para obter mais informações, consulte [Conectar-se à instância do Linux em caso de perda da chave privada \(p. 1220\)](#).
3. Conecte-se à instância usando o novo par de chaves.

## Erro: Chave do usuário não reconhecida pelo servidor

Se você usar o SSH para conectar à sua instância

- Use `ssh -vvv` para obter o triplo de informações de depuração detalhadas (verbose) ao se conectar:

```
ssh -vvv -i path/my-key-pair.pem my-instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

O exemplo de saída a seguir demonstra o que você pode ver se estivesse tentando se conectar à sua instância com uma chave não reconhecida pelo servidor:

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: key_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
```

```
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Se você usar o PuTTY para se conectar à instância

- Verifique se o arquivo de chave privada (.pem) foi convertido para o formato reconhecido pelo PuTTY (.ppk). Para obter mais informações sobre a conversão da sua chave privada, consulte [Conectar-se à instância do Linux no Windows usando PuTTY \(p. 552\)](#).

Note

No PuTTYgen, carregue o arquivo de chave privada e selecione Salvar chave privada em vez de Gerar.

- Verifique se você está se conectando com o nome de usuário adequado para sua AMI. Insira o nome de usuário na caixa Nome do host na janela Configuração do PuTTY.
  - Para o Amazon Linux 2 ou a AMI do Amazon Linux, o nome do usuário é `ec2-user`.
  - Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
  - Para uma AMI do Ubuntu, o nome do usuário é `admin`.
  - Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
  - Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.
  - Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.
  - Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
  - Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
  - Para uma AMI do Bitnami, o nome do usuário é `bitnami`.
  - Caso contrário, verifique com o provedor da AMI.
- Verifique se você tem uma regra do security group de entrada para permitir tráfego de entrada para a porta apropriada. Para mais informações, consulte [Autorização de acesso de rede para suas instâncias \(p. 1205\)](#).

## Erro: permissão negada ou conexão fechada pela porta 22 de [instância]

Se você se conectar à instância usando SSH e obtiver algum dos erros `Host key not found in [directory]`, `Permission denied (publickey)`, `Authentication failed, permission denied` ou `Connection closed by [instance] port 22`, verifique se está se conectando com o nome de usuário apropriado para a AMI e se especificou o arquivo de chave privada (.pem) apropriado para a instância.

Os nomes de usuários apropriados são os seguintes:

- Para o Amazon Linux 2 ou a AMI do Amazon Linux, o nome do usuário é `ec2-user`.
- Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
- Para uma AMI do Ubuntu, o nome do usuário é `admin`.
- Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
- Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
- Para uma AMI do Bitnami, o nome do usuário é `bitnami`.

- 
- Caso contrário, verifique com o provedor da AMI.

Por exemplo, para usar um cliente SSH para se conectar a uma instância do Amazon Linux, use o seguinte comando:

```
ssh -i /path/my-key-pair.pem my-instance-user-name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Confirme se você está usando um arquivo de chave privada que corresponde ao par de chaves que selecionou ao executar a instância.

#### New console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instances (Instâncias) e, em seguida, selecione sua instância.
3. Na guia Details (Detalhes), em Instance details (Detalhes da instância), verifique o valor do Nome do par de chaves.
4. Se você não tiver especificado um par de chaves ao executar a instância, pode encerrar a instância e executar uma nova, especificando um par de chaves. Se essa for uma instância que você está usando mas não tiver mais o arquivo .pem para seu par de chaves, pode substituir o par de chaves por um novo. Para obter mais informações, consulte [Conectar-se à instância do Linux em caso de perda da chave privada \(p. 1220\)](#).

#### Old console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação, selecione Instances (Instâncias) e, em seguida, selecione sua instância.
3. Na guia Descrição, verifique o valor de Nome do par de chaves.
4. Se você não tiver especificado um par de chaves ao executar a instância, pode encerrar a instância e executar uma nova, especificando um par de chaves. Se essa for uma instância que você está usando mas não tiver mais o arquivo .pem para seu par de chaves, pode substituir o par de chaves por um novo. Para obter mais informações, consulte [Conectar-se à instância do Linux em caso de perda da chave privada \(p. 1220\)](#).

Se você tiver gerado seu próprio par de chaves, garanta que o gerador de chaves está configurado para criar chaves RSA. Chaves DSA não são aceitas.

Se você obtiver um erro `Permission denied (publickey)` e nenhum dos casos acima se aplicar (por exemplo, você conseguiu se conectar previamente), as permissões no diretório inicial da sua instância podem ter sido alteradas. As permissões para `/home/my-instance-user-name/.ssh/authorized_keys` devem ser limitadas somente ao proprietário.

#### Para verificar as permissões na sua instância

1. Pare sua instância e separe o volume do dispositivo raiz. Para obter mais informações, consulte [Interromper e iniciar sua instância \(p. 562\)](#) e [Desanexar um volume do Amazon EBS de uma instância Linux \(p. 1300\)](#).
2. Execute uma instância temporária na mesma zona de disponibilidade que sua instância atual (use uma AMI semelhante ou a mesma AMI usada para sua instância atual) e associe o volume do dispositivo raiz à instância temporária. Para obter mais informações, consulte [Vincular um volume do Amazon EBS a uma instância \(p. 1277\)](#).
3. Conecte-se à instância temporária, crie um ponto de montagem e monte o volume associado. Para obter mais informações, consulte [Disponibilizar um volume do Amazon EBS para uso no Linux \(p. 1283\)](#).

4. Na instância temporária, verifique as permissões do diretório `/home/my-instance-user-name/` do volume associado. Se necessário, ajuste as permissões da seguinte forma:

```
[ec2-user ~]$ chmod 600 mount_point/home/my-instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/my-instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/my-instance-user-name
```

5. Desmonte o volume, separe-o da instância temporária e reassocie-o à instância original. Especifique o nome correto do dispositivo para o volume do dispositivo raiz; por exemplo, `/dev/xvda`.
6. Execute sua instância. Se você não precisar mais da instância temporária, pode encerrá-la.

## Erro: arquivo de chave privada desprotegido

Seu arquivo de chave privada deve estar protegido contra operações de leitura e gravação por parte de qualquer outro usuário. Se sua chave privada puder ser lida ou gravada por qualquer pessoa menos você, o SSH ignorará sua chave e você verá a mensagem de advertência abaixo.

```
@@@@@@@WARNING: UNPROTECTED PRIVATE KEY FILE!@@@@@@@  
@Permissions 0777 for '.ssh/my_private_key.pem' are too open.  
It is required that your private key files are NOT accessible by others.  
This private key will be ignored.  
bad permissions: ignore key: .ssh/my_private_key.pem  
Permission denied (publickey).
```

Se você vir uma mensagem semelhante ao tentar fazer login na sua instância, examine a primeira linha da mensagem de erro para verificar se está usando a chave pública correta para sua instância. O exemplo acima usa a chave privada `.ssh/my_private_key.pem` com permissões de arquivo 0777, que permitem que qualquer pessoa leia ou grave nesse arquivo. O nível de permissão é muito inseguro, por isso o SSH ignora essa chave.

Se você está se conectando do MacOS ou do Linux, execute o comando a seguir para corrigir esse erro, substituindo o caminho para o arquivo de chave privada.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Se você estiver se conectando do Windows, execute as etapas a seguir no computador local.

1. Navegue até o arquivo `.pem`.
2. Clique com o botão direito do mouse no arquivo `.pem` e selecione Properties (Propriedades).
3. Escolha a guia Segurança.
4. Selecione Advanced (Avançado).
5. Verifique se você é o proprietário do arquivo. Caso contrário, altere o proprietário para seu nome de usuário.
6. Selecione Disable inheritance (Desabilitar herança) e Remove all inherited permissions from this object (Remover todas as permissões herdadas deste objeto).
7. Selecione Add (Adicionar), Select a principal (Selecionar um principal), insira seu nome de usuário e selecione OK.
8. Na janela Permission Entry (Entrada de permissão), conceda as permissões Read (Leitura) e selecione OK.

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
Erro: a chave privada deve começar com "----  
BEGIN RSA PRIVATE KEY----" e terminar

- 
9. Selecione OK para fechar a janela **Advanced Private Key Settings** (Configurações avançadas de segurança).
  10. Selecione OK para fechar a janela Properties (Propriedades).
  11. Você deve ser capaz de se conectar à instância Linux no Windows por meio de SSH.

No prompt de comando do Windows, execute os comandos a seguir.

1. No prompt de comando, navegue até o local do caminho do arquivo .pem.
2. Execute o seguinte comando para redefinir e remover permissões explícitas:

```
icacls.exe $path /reset
```

3. Execute o seguinte comando para conceder permissões de leitura ao usuário atual:

```
icacls.exe $path /GRANT:R "$(env:USERNAME):(R)"
```

4. Execute o seguinte comando para desabilitar a herança e remover permissões herdadas.

```
icacls.exe $path /inheritance:r
```

5. Você deve ser capaz de se conectar à instância Linux no Windows por meio de SSH.

## Erro: a chave privada deve começar com "----BEGIN RSA PRIVATE KEY----" e terminar com "----END RSA PRIVATE KEY----"

Se usar uma ferramenta de terceiros, como ssh-keygen, para criar um par de chaves RSA, ela gerará a chave privada no formato de chave OpenSSH. Quando você se conecta à sua instância, se você usar a chave privada no formato OpenSSH para descriptografar a senha, você receberá o erro `Private key must begin with "----BEGIN RSA PRIVATE KEY----" and end with "----END RSA PRIVATE KEY----"`.

Para resolver o erro, a chave privada deve estar no formato PEM. Use o comando a seguir para criar a chave privada no formato PEM:

```
ssh-keygen -m PEM
```

## Erro: o servidor recusou nossa chave ou não há métodos de autenticação compatíveis disponíveis

Se você usar o PuTTY para se conectar à instância e obtiver algum dos erros a seguir, Erro: o servidor recusou nossa chave ou Erro: não há métodos de autenticação compatíveis, verifique se está se conectando com o nome de usuário apropriado para a AMI. Digite o nome de usuário em Nome do usuário na janela Configuração do PuTTY.

Os nomes de usuários apropriados são os seguintes:

- Para o Amazon Linux 2 ou a AMI do Amazon Linux, o nome do usuário é `ec2-user`.
- Para uma AMI do CentOS, o nome do usuário é `centos` ou `ec2-user`.
- Para uma AMI do Ubuntu, o nome do usuário é `admin`.

- Para uma AMI do Fedora, o nome do usuário é `fedora` ou `ec2-user`.
- Para uma AMI do RHEL, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do SUSE, o nome do usuário é `ec2-user` ou `root`.
- Para uma AMI do Ubuntu, o nome de usuário é `ubuntu`.
- Para uma AMI do Oracle, o nome do usuário é `ec2-user`.
- Para uma AMI do Bitnami, o nome do usuário é `bitnami`.
- Caso contrário, verifique com o provedor da AMI.

Você também deve verificar se o arquivo de chave privada (`.pem`) foi convertido corretamente para o formato reconhecido pelo PuTTY (`.ppk`). Para obter mais informações sobre a conversão da sua chave privada, consulte [Conectar-se à instância do Linux no Windows usando PuTTY](#) (p. 552).

## Não é possível fazer o ping da instância

O comando `ping` é um tipo de tráfego de ICMP — se você não conseguir fazer o ping da sua instância, verifique se as regras do grupo de segurança de entrada permitem tráfego de ICMP para a mensagem `Echo Request` de todas as origens, ou do computador ou da instância em que você está emitindo o comando.

Caso você não consiga emitir um comando `ping` por sua instância, assegure-se de que suas regras do security group de saída permitam tráfego de ICMP para a mensagem `Echo Request` a todos os destinos ou para o host no qual você está tentando fazer o ping.

`Ping`Os comandos também podem ser bloqueados por um firewall ou tempo de espera devido a problemas de latência de rede ou hardware. Você deve consultar o administrador de sistema ou de rede local para obter ajuda com mais solução de problemas.

## Erro: Server unexpectedly closed network connection (A conexão de rede foi fechada inesperadamente pelo servidor)

Se você estiver se conectando à instância com o PuTTY e receber o erro "A conexão de rede foi fechada inesperadamente pelo servidor", verifique se os keepalives estão habilitados na página Conexão da Configuração do PuTTY para evitar ser desconectado. Alguns servidores desconectam clientes quando eles não recebem nenhum dado em determinado período. Defina os segundos entre os keepalives para 59 segundos.

Se você ainda tiver problemas após habilitar os keepalives, tente desabilitar o algoritmo de Nagle na página Conexão da Configuração do PuTTY.

## Erro: falha na validação da chave do host para EC2 Instance Connect

Se você alternar as chaves do host da instância, as novas chaves do host não serão automaticamente carregadas para o banco de dados de chaves de host confiáveis da AWS. Isso faz com que a validação da chave do host apresente falha quando você tenta se conectar à instância usando o cliente EC2 Instance Connect baseado em navegador e você não consegue se conectar à instância.

Para resolver o erro, você deve executar o script `eic_harvest_hostkeys` na instância, o que carregará sua nova chave de host para EC2 Instance Connect. O script está localizado em `/opt/aws/bin/` nas instâncias do Amazon Linux 2 e em `/usr/share/ec2-instance-connect/` nas instâncias do Ubuntu.

Para resolver o erro de falha de validação da chave de host em uma instância do Amazon Linux 2.

1. Conecte-se à sua instância usando SSH.

Faça a conexão usando a CLI EC2 Instance Connect ou o par de chaves de SSH atribuído à instância quando você a executou e o nome do usuário padrão da AMI usada para executar a instância. Para Amazon Linux 2, o nome do usuário padrão é `ec2-user`.

Por exemplo, se a instância tiver sido executada usando o Amazon Linux 2, o nome DNS público da instância for `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e o par de chaves for `my_ec2_private_key.pem`, use o seguinte comando para o SSH na instância:

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Para obter mais informações sobre como se conectar à sua instância, consulte [Conectar-se à instância do Linux usando SSH \(p. 538\)](#).

2. Navegue até a seguinte pasta.

```
[ec2-user ~]$ cd /opt/aws/bin/
```

3. Execute o seguinte comando na sua instância.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Observe que uma chamada bem-sucedida não resulta em saída.

Agora você pode usar o cliente EC2 Instance Connect baseado em navegador para se conectar à instância.

## Ubuntu

Para resolver o erro de falha de validação da chave de host em uma instância do Ubuntu

1. Conecte-se à sua instância usando SSH.

Faça a conexão usando a CLI EC2 Instance Connect ou o par de chaves de SSH atribuído à instância quando você a executou e o nome do usuário padrão da AMI usada para executar a instância. Para Ubuntu, o nome de usuário padrão é `ubuntu`.

Por exemplo, se a instância tiver sido executada usando o Ubuntu, o nome DNS público da instância for `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` e o nome do par de chaves for `my_ec2_private_key.pem`, use o seguinte comando para o SSH na instância:

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-west-2.compute.amazonaws.com
```

Para obter mais informações sobre como se conectar à sua instância, consulte [Conectar-se à instância do Linux usando SSH \(p. 538\)](#).

2. Navegue até a seguinte pasta.

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Execute o seguinte comando na sua instância.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Observe que uma chamada bem-sucedida não resulta em saída.

Agora você pode usar o cliente EC2 Instance Connect baseado em navegador para se conectar à 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 (Imagem 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 Linux a partir de uma instância \(p. 108\)](#).

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 Linux a partir de uma instância \(p. 108\)](#).

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 forçará o encerramento dela dali 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 \(p. 1570\)](#) 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 \(p. 700\)](#) ou [Criar uma solicitação de frota spot \(p. 764\)](#).

## Solução de problemas em instâncias com falha nas verificações de status

As informações a seguir podem ajudá-lo a solucionar problemas se sua instância falhar em uma verificação de status. Determine primeiro se seus aplicativos exibem quaisquer problemas. Se você verificar que a instância não está executando seus aplicativos como esperado, analise as informações de verificação de status e os logs do sistema.

Para obter exemplos de problemas que podem causar falha nas verificações de status, consulte [Verificações de status para as instâncias \(p. 841\)](#).

### Tópicos

- [Analizar informações de verificação de status \(p. 1587\)](#)

- Recuperar os logs do sistema (p. 1588)
- Solução de problemas de erros de logs do sistema para instâncias baseadas em Linux (p. 1588)
- Sem memória: encerrar processo (p. 1589)
- ERRO: falha em mmu\_update (falha na atualização do gerenciamento de memória) (p. 1590)
- Erro de E/S (falha de dispositivo de blocos) (p. 1591)
- ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado) (p. 1592)
- request\_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux) (p. 1593)
- "FATAL: kernel antigo demais" e "fsck: Não existe esse arquivo ou diretório ao tentar abrir /dev" (falta de correspondência entre o kernel e a AMI) (p. 1594)
- "FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes) (p. 1594)
- ERRO Kernel inválido (kernel incompatível com EC2) (p. 1595)
- fsck: Nenhum arquivo ou diretório ao tentar abrir... (Sistema de arquivos não encontrado) (p. 1596)
- Erro geral ao montar os sistemas de arquivos (falha na montagem) (p. 1598)
- VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz) (p. 1599)
- Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz) (p. 1600)
- XENBUS: Dispositivo sem driver... (p. 1601)
- ...dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos) (p. 1602)
- O fsck morreu com status de saída... (Dispositivo ausente) (p. 1603)
- Prompt do GRUB (grubdom>) (p. 1604)
- Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded) (p. 1606)
- Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux) (p. 1607)
- XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus) (p. 1608)

## Analizar informações de verificação de status

Para investigar instâncias prejudicadas 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, em seguida, sua instância.
3. No painel de detalhes, escolha Verificações de status para ver os resultados individuais de todas as Verificações de status do sistema e as Verificações de status da instância.

Se uma verificação do status do sistema falhar, você pode tentar uma das opções a seguir:

- Crie um alarme de recuperação da instância. Para obter mais informações, consulte [Criar alarmes para interromper, encerrar, reiniciar ou recuperar uma instância \(p. 898\)](#).
- Se você alterou o tipo de instância para uma instância criada no [Sistema Nitro \(p. 210\)](#), as verificações de status falharão se você tiver migrado de uma instância que não possui os drivers ENA e NVMe necessários. Para obter mais informações, consulte [Compatibilidade para alterar o tipo de instância \(p. 328\)](#).

- Para uma instância usando AMI com Amazon EBS, pare e reinicie a instância.
- Para uma instância usando uma AMI com armazenamento de instâncias, encerre a instância e execute uma substituição.
- Espere o Amazon EC2 resolver o problema.
- Publique seu problema no [fórum do Amazon EC2](#).
- Se sua instância está em um grupo do Auto Scaling, o serviço do Amazon EC2 Auto Scaling executa uma instância de substituição automaticamente. Para obter mais informações, consulte [Verificações de integridade de instâncias do Auto Scaling](#) no Guia do usuário do Amazon EC2 Auto Scaling.
- Recupere o log do sistema e procure erros.

## Recuperar os logs do sistema

Se uma verificação de status da instância falhar, você poderá reinicializar a instância e recuperar os logs do sistema. Os logs podem revelar um erro que pode ajudar você a resolver o problema. Reiniciar limpa as informações desnecessária dos logs.

Para reinicializar uma instância e recuperar o log do sistema

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) e Reboot instance (Reiniciar instância). Pode demorar alguns minutos para a instância reinicializar.
4. Verifique o problema ainda existe; em alguns casos, reinicializar pode resolver o problema.
5. Quando a ação estiver no estado `running`, escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log (Obter log do sistema).
6. Revise o log que aparece na tela e use a lista de declarações conhecidas de erro do log do sistema, abaixo, para solucionar seu problema.
7. Se sua experiência diferir dos resultados de verificação, ou se estiver com problemas com sua instância que nossas verificações não detectaram, escolha Enviar feedback na guia Verificações de status para nos ajudar a melhorar os testes de detecção.
8. Se seu problema não for resolvido, você pode publicá-lo no [fórum do Amazon EC2](#).

## Solução de problemas de erros de logs do sistema para instâncias baseadas em Linux

Para instâncias baseadas em Linux que reprovaram em uma verificação de status da instância, como a verificação de acessibilidade da instância, verifique se você seguiu as etapas acima para recuperar o log do sistema. A lista a seguir contém alguns erros comuns no log do sistema e ações sugeridas que você pode utilizar para resolver o problema de cada erro.

Erros de memória

- [Sem memória: encerrar processo \(p. 1589\)](#)
- [ERRO: falha em mmu\\_update \(falha na atualização do gerenciamento de memória\) \(p. 1590\)](#)

Erros do dispositivo

- [Erro de E/S \(falha de dispositivo de blocos\) \(p. 1591\)](#)
- [ERRO DE E/S: nem disco local nem disco remoto \(o dispositivo de blocos distribuído está quebrado\) \(p. 1592\)](#)

### Erros de kernel

- request\_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux) (p. 1593)
- "FATAL: kernel antigo demais" e "fsck: Não existe esse arquivo ou diretório ao tentar abrir /dev" (falta de correspondência entre o kernel e a AMI) (p. 1594)
- "FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes) (p. 1594)
- ERRO Kernel inválido (kernel incompatível com EC2) (p. 1595)

### Erros do sistema de arquivos

- fsck: Nenhum arquivo ou diretório ao tentar abrir... (Sistema de arquivos não encontrado) (p. 1596)
- Erro geral ao montar os sistemas de arquivos (falha na montagem) (p. 1598)
- VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz) (p. 1599)
- Erro: não foi possível determinar o número principal/secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz) (p. 1600)
- XENBUS: Dispositivo sem driver... (p. 1601)
- ...dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos) (p. 1602)
- O fsck morreu com status de saída... (Dispositivo ausente) (p. 1603)

### Erros do sistema operacional

- Prompt do GRUB (grubdom>) (p. 1604)
- Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded) (p. 1606)
- Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux) (p. 1607)
- XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus) (p. 1608)

## Sem memória: encerrar processo

O erro de falta de memória é indicado por uma entrada no log de sistema semelhante à exibida abaixo.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

### Possível causa

Memória exaurida

### Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Execute um destes procedimentos:

Para este tipo de instância	Faça o seguinte
	<ul style="list-style-type: none"><li>Pare a instância, modifique-a para usar um tipo de instância diferente e inicie-a novamente. Por exemplo, um tipo de instância maior ou otimizado para memória.</li><li>Reinicialize a instância para ela retornar ao status não prejudicado. O problema provavelmente ocorrerá outra vez, a menos que você altere o tipo de instância.</li></ul>
Com armazenamento de instâncias	<p>Execute um destes procedimentos:</p> <ul style="list-style-type: none"><li>Encerre a instância e execute uma nova instância, especificando um tipo de instância diferente. Por exemplo, um tipo de instância maior ou otimizado para memória.</li><li>Reinicialize a instância para ela retornar ao status não prejudicado. O problema provavelmente ocorrerá outra vez, a menos que você altere o tipo de instância.</li></ul>

## ERRO: falha em mmu\_update (falha na atualização do gerenciamento de memória)

As falhas de atualização do gerenciamento de memória são indicadas por uma entrada no log do sistema semelhante à seguinte:

```
...
Press `ESC' to enter the menu... 0      [H[J  Booting 'Amazon Linux 2011.09
(2.6.35.14-95.38.amzn1.i686)'

root (hd0)

Filesystem type is ext2fs, using whole disk

kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=
en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

### Possível causa

Problema com Amazon Linux

### Ação sugerida

Publique seu problema nos [Fóruns de desenvolvedores](#) ou entre em contato com o [AWS Support](#).

## Erro de E/S (falha de dispositivo de blocos)

Um erro de entrada/saída é indicado por uma entrada no log do sistema semelhante ao exemplo a seguir:

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
...
```

## Possíveis causas

Tipo de instância	Possível causa
Baseado em Amazon EBS	Um volume do Amazon EBS com falha
Com armazenamento de instâncias	Uma unidade física com falha

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>1. Pare a instância.</li><li>2. Separe o volume.</li><li>3. Tentativa de recuperar o volume.</li></ol> <p>Note</p> <p>É boa prática tirar um snapshot dos seus volumes do Amazon EBS com frequência. Isso diminui drasticamente o risco de perda de dados como resultado da falha.</p> <ol style="list-style-type: none"><li>4. Reassocie o volume à instância.</li><li>5. Inicie a instância.</li></ol>
Com armazenamento de instâncias	Encerre a instância e execute uma nova instância.

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
**ERRO DE E/S: nem disco local nem disco remoto  
(o dispositivo de blocos distribuído está quebrado)**

Para este tipo de instância	Faça o seguinte
	<p>Note</p> <p>Os dados não podem ser recuperados. Recupere os backups.</p> <p>Note</p> <p>É uma boa prática usar Amazon S3 ou Amazon EBS para backup. Os volumes de armazenamento de instâncias estão diretamente vinculados a um único host e a falhas únicas de disco.</p>

## ERRO DE E/S: nem disco local nem disco remoto (o dispositivo de blocos distribuído está quebrado)

Um erro de entrada/saída no dispositivo é indicado por uma entrada no log do sistema semelhante ao exemplo a seguir:

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...
Aborting journal on device drbd1-8.
block drbd1: IO ERROR: neither local nor remote disk
Buffer I/O error on device drbd1, logical block 557056
lost page write due to I/O error on drbd1
JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

### Possíveis causas

Tipo de instância	Possível causa
Baseado em Amazon EBS	Um volume do Amazon EBS com falha
Com armazenamento de instâncias	Uma unidade física com falha

### Ação sugerida

Encerre a instância e execute uma nova instância.

Para uma instância com Amazon EBS, você pode recuperar os dados de um snapshot recente ao criar uma imagem a partir de deles. Alguns dados adicionados depois do snapshot não podem ser recuperados.

## request\_module: modprobe de loop descontrolado (modprobe do kernel legado do looping, em versões mais antigas do Linux)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo. Usar um kernel instável ou antigo do Linux (por exemplo, 2.6.16-xenU) pode causar uma condição de loop interminável na inicialização.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1  
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007  
  
BIOS-provided physical RAM map:  
  
Xen: 0000000000000000 - 0000000026700000 (usable)  
  
0MB HIGHMEM available.  
...  
  
request_module: runaway loop modprobe binfmt-464c  
  
request_module: runaway loop modprobe binfmt-464c
```

### Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Use um kernel mais novo, baseado em GRUB ou estático, usando uma das seguintes opções:</p> <p>Opção 1: Encerre a instância e execute uma nova, especificando os parâmetros <code>-kernel</code> e <code>-ramdisk</code>.</p> <p>Opção 2:</p> <ol style="list-style-type: none"><li>1. Pare a instância.</li><li>2. Modifique os atributos de kernel e ramdisk para usar um kernel mais recente.</li><li>3. Inicie a instância.</li></ol>
Com armazenamento de instâncias	Encerre a instância e execute uma nova, especificando os parâmetros <code>-kernel</code> e <code>-ramdisk</code> .

## "FATAL: kernel antigo demais" e "fsck: Não existe esse arquivo ou diretório ao tentar abrir /dev" (falta de correspondência entre o kernel e a AMI)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

### Possíveis causas

Kernel e userland incompatíveis

### Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>1. Pare a instância.</li><li>2. Modifique a configuração para usar um kernel mais recente.</li><li>3. Inicie a instância.</li></ol>
Com armazenamento de instâncias	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>1. Crie uma AMI que use um kernel mais recente.</li><li>2. Encerre a instância.</li><li>3. Execute uma nova instância com base na AMI criada.</li></ol>

## "FATAL: Não foi possível carregar os módulos /lib/" ou "BusyBox" (módulos do kernel ausentes)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No such
file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
Done.
Begin: Running /scripts/init-premount ...
Done.
```

```
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device. Common problems:
- Boot args (cat /proc/cmdline)
- Check rootdelay= (did the system wait long enough?)
- Check root= (did the system wait for the right device?)
- Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or directory
ALERT! /dev/sdal does not exist. Dropping to a shell!

BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

## Possíveis causas

Uma ou mais das condições a seguir podem causar esse problema:

- Ramdisk ausente
- Módulos corretos do ramdisk ausentes
- Volume do dispositivo raiz do Amazon EBS não associado corretamente como /dev/sda1

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>1. Selecione o ramdisk corrigido para o volume do Amazon EBS.</li><li>2. Pare a instância.</li><li>3. Desanexe o volume e repare-o.</li><li>4. Associe o volume à instância.</li><li>5. Inicie a instância.</li><li>6. Modifique a AMI para usar o ramdisk corrigido.</li></ol>
Com armazenamento de instâncias	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>1. Encerre a instância e execute uma nova instância com o ramdisk correto.</li><li>2. Crie uma nova AMI com o ramdisk correto.</li></ol>

## ERRO Kernel inválido (kernel incompatível com EC2)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
...
root (hd0)
```

```
Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img

ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

Booting 'Fallback'

root (hd0)

Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

## Possíveis causas

Uma ou ambas as condições a seguir podem causar esse problema:

- O kernel fornecido não é compatível com GRUB
- O kernel de fallback não existe

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	Use o procedimento a seguir: <ol style="list-style-type: none"><li>1. Pare a instância.</li><li>2. Substitua por um kernel em funcionamento.</li><li>3. Instale um kernel de fallback.</li><li>4. Modifique a AMI corrigindo o kernel.</li></ol>
Com armazenamento de instâncias	Use o procedimento a seguir: <ol style="list-style-type: none"><li>1. Encerre a instância e execute uma nova instância com o kernel correto.</li><li>2. Crie uma AMI com o kernel correto.</li><li>3. (Opcional) Procure assistência técnica para recuperação de dados usando o <a href="#">AWS Support</a>.</li></ol>

## fsck: Nenhum arquivo ou diretório ao tentar abrir... (Sistema de arquivos não encontrado)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
Welcome to Fedora
```

Amazon Elastic Compute Cloud Manual  
do usuário para instâncias do Linux  
fsck: Nenhum arquivo ou diretório ao tentar  
abrir... (Sistema de arquivos não encontrado)

```
Press 'I' to enter interactive startup.  
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [ OK ]  
  
Starting udev: [ OK ]  
  
Setting hostname localhost: [ OK ]  
  
No devices found  
Setting up Logical Volume Management: File descriptor 7 left open  
    No volume groups found  
[ OK ]  
  
Checking filesystems  
Checking all file systems.  
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1  
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks  
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh  
fsck.ext3: No such file or directory while trying to open /dev/sdh  
  
/dev/sdh:  
The superblock could not be read or does not describe a correct ext2  
filesystem. If the device is valid and it really contains an ext2  
filesystem (and not swap or ufs or something else), then the superblock  
is corrupt, and you might try running e2fsck with an alternate superblock:  
    e2fsck -b 8193 <device>  
  
[FAILED]  
  
*** An error occurred during the file system check.  
*** Dropping you to a shell; the system will reboot  
*** when you leave the shell.  
Give root password for maintenance  
(or type Control-D to continue):
```

## Possíveis causas

- Existe um bug nas definições de /etc/fstab do sistema de arquivos do ramdisk
- Definições do sistema de arquivos com configuração errada em /etc/fstab
- Unidade ausente/com falha

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>1. Pare a instância, separe o volume do dispositivo raiz, repare/modifique /etc/fstab o volume, associe o volume à instância e inicie a instância.</li><li>2. Corrija o ramdisk para incluir o /etc/fstab modificado (se aplicável).</li><li>3. Modifique as AMIs para usar um ramdisk mais recente.</li></ol> <p>O sexto campo do fstab define os requisitos de disponibilidade da montagem – um valor diferente</p>

Para este tipo de instância	Faça o seguinte
	de zero implica que um fsck será feito nesse volume e deve ter sucesso. Usar esse campo pode ser problemático no Amazon EC2, pois a falha tipicamente resulta em um prompt do console interativo que não está disponível atualmente no Amazon EC2. Tenha cuidado com esse recurso e leia a man page do Linux para fstab.
Com armazenamento de instâncias	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"> <li>1. Encerre a instância e execute uma nova instância.</li> <li>2. Separe todos os volumes do Amazon EBS com erro e a instância de reinicialização.</li> <li>3. (Opcional) Procure assistência técnica para recuperação de dados usando o <a href="#">AWS Support</a>.</li> </ol>

## Erro geral ao montar os sistemas de arquivos (falha na montagem)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```

Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting. Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):

```

## Possíveis causas

Tipo de instância	Possível causa
Baseado em Amazon EBS	<ul style="list-style-type: none"> <li>Volume do Amazon EBS destacado ou com falha.</li> <li>Sistema de arquivos corrompido.</li> <li>Combinação malfeita de ramdisk e AMI (por exemplo, ramdisk Debian com AMI SUSE).</li> </ul>
Com armazenamento de instâncias	<ul style="list-style-type: none"> <li>Uma unidade com falha.</li> <li>Um sistema de arquivos corrompido.</li> <li>Combinação malfeita de ramdisk e AMI (por exemplo, ramdisk Debian com AMI SUSE).</li> </ul>

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"> <li>Pare a instância.</li> <li>Separar o volume de raiz.</li> <li>Associe o volume do dispositivo raiz a uma instância de trabalho conhecida.</li> <li>Execute uma verificação no sistema de arquivos (fsck -a /dev/...).</li> <li>Corrija todos os erros.</li> <li>Separar o volume de instância de trabalho conhecida.</li> <li>Associe o volume à instância parada.</li> <li>Inicie a instância.</li> <li>Verifique novamente o status da instância.</li> </ol>
Com armazenamento de instâncias	<p>Faça uma das coisas a seguir:</p> <ul style="list-style-type: none"> <li>Execute uma nova instância.</li> <li>(Opcional) Procure assistência técnica para recuperação de dados usando o <a href="#">AWS Support</a>.</li> </ul>

## VFS: Não foi possível montar o fs raiz em um bloco desconhecido (falta de correspondência no sistema de arquivos-raiz)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

Erro: não foi possível determinar o número principal/  
secundário do dispositivo raiz... (Incompatibilidade  
entre sistema de arquivos/dispositivo raiz)

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line: root=/dev/sdal ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

## Possíveis causas

Tipo de instância	Possível causa
Baseado em Amazon EBS	<ul style="list-style-type: none"> <li>Dispositivo não associado corretamente.</li> <li>O dispositivo raiz não foi associado no ponto correto do dispositivo.</li> <li>O sistema de arquivos não está no formato esperado.</li> <li>Uso do kernel de legado (por exemplo, 2.6.16-XenU).</li> <li>Uma atualização de kernel recente na sua instância (atualização defeituosa ou bug de atualização)</li> </ul>
Com armazenamento de instâncias	Falha no dispositivo de hardware.

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Execute um destes procedimentos:</p> <ul style="list-style-type: none"> <li>Pare e reinicie a instância.</li> <li>Modifique o volume do dispositivo raiz para associar no ponto correto do dispositivo, possível /dev/sda1 em vez de /dev/sda.</li> <li>Pare e modifique para usar o kernel moderno.</li> <li>Consulte a documentação para sua distribuição Linux para verificar bugs conhecidos da atualização. Altere ou reinstale o kernel.</li> </ul>
Com armazenamento de instâncias	Encerre a instância e execute uma nova instância usando um kernel moderno.

## Erro: não foi possível determinar o número principal/ secundário do dispositivo raiz... (Incompatibilidade entre sistema de arquivos/dispositivo raiz)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs/]#
```

## Possíveis causas

- Driver do dispositivo de blocos virtual ausente ou configurado incorretamente
- Conflito de enumeração de dispositivos (sda versus xvda ou sda em vez de sda1)
- Escolha incorreta do kernel da instância

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>1. Pare a instância.</li><li>2. Separe o volume.</li><li>3. Corrija o problema de mapeamento de dispositivos.</li><li>4. Inicie a instância.</li><li>5. Modifique a AMI para abordar os problemas de mapeamento de dispositivos.</li></ol>
Com armazenamento de instâncias	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>1. Crie nova AMI com a correção apropriada (mapeie o dispositivo de blocos corretamente).</li><li>2. Encerre a instância e execute uma nova a partir da AMI criada.</li></ol>

## XENBUS: Dispositivo sem driver...

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
```

```
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs/]#
```

## Possíveis causas

- Driver do dispositivo de blocos virtual ausente ou configurado incorretamente
- Conflito de enumeração de dispositivos (sda versus xvda)
- Escolha incorreta do kernel da instância

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"> <li>1. Pare a instância.</li> <li>2. Separe o volume.</li> <li>3. Corrija o problema de mapeamento de dispositivos.</li> <li>4. Inicie a instância.</li> <li>5. Modifique a AMI para abordar os problemas de mapeamento de dispositivos.</li> </ol>
Com armazenamento de instâncias	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"> <li>1. Crie uma AMI com a correção apropriada (mapeie o dispositivo de blocos corretamente).</li> <li>2. Encerre a instância e execute uma nova usando a AMI criada.</li> </ol>

## ...dias sem ser verificada, verificação forçada (verificação necessária para o sistema de arquivos)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

## Possíveis causas

Tempo de verificação do sistema de arquivos passado; uma verificação do sistema de arquivos está sendo forçada.

## Ações sugeridas

- Espere até que a verificação do sistema de arquivos seja concluída. Uma verificação do sistema de arquivos pode demorar bastante, dependendo do tamanho do sistema de arquivos raiz.
- Modifique seus sistemas de arquivos para remover a obrigatoriedade de verificação do sistema de arquivos (fsck) usando tune2fs ou ferramentas apropriadas para seu sistema de arquivos.

## O fsck morreu com status de saída... (Dispositivo ausente)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
Cleaning up ifupdown....  
Loading kernel modules...done.  
...  
Activating lvm and md swap...done.  
Checking file systems...fsck from util-linux-ng 2.16.2  
/sbin/fsck.xfs: /dev/sdh does not exist  
fsck died with exit status 8  
[31mfailed (code 8).[39;49m
```

## Possíveis causas

- Ramdisk procurando unidade ausente
- Verificação de consistência do sistema de arquivos forçada
- Unidade falha ou separada

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Teste uma ou mais das opções a seguir para resolver o problema:</p> <ul style="list-style-type: none"><li>• Pare a instância, associe o volume a uma instância em execução existente.</li><li>• Execute manualmente verificações de consistência.</li><li>• Conserte o ramdisk para incluir utilitários relevantes.</li><li>• Modifique os parâmetros de ajuste do sistema de arquivos para remover os requisitos de consistência (não recomendados).</li></ul>
Com armazenamento de instâncias	<p>Teste uma ou mais das opções a seguir para resolver o problema:</p>

Para este tipo de instância	Faça o seguinte
	<ul style="list-style-type: none"><li>• Reempacote o ramdisk com as ferramentas corretas.</li><li>• Modifique os parâmetros de ajuste do sistema de arquivos para remover os requisitos de consistência (não recomendados).</li><li>• Encerre a instância e execute uma nova instância.</li><li>• (Opcional) Procure assistência técnica para recuperação de dados usando o <a href="#">AWS Support</a>.</li></ul>

## Prompt do GRUB (grubdom>)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
GNU GRUB version 0.97 (629760K lower / 0K upper memory)

[ Minimal BASH-like line editing is supported. For
the first word, TAB lists possible command
completions. Anywhere else TAB lists the possible
completions of a device/filename. ]

grubdom>
```

## Possíveis causas

Tipo de instância	Possíveis causas
Baseado em Amazon EBS	<ul style="list-style-type: none"><li>• Arquivo de configuração do GRUB ausente.</li><li>• Imagem incorreta de GRUB usada, esperando arquivo de configuração do GRUB em um local diferente.</li><li>• Sistema de arquivos não compatível usado para armazenar seu arquivo de configuração de GRUB (por exemplo, convertendo o sistema de arquivos raiz a um tipo que não é compatível com uma versão anterior do GRUB).</li></ul>
Com armazenamento de instâncias	<ul style="list-style-type: none"><li>• Arquivo de configuração do GRUB ausente.</li><li>• Imagem incorreta de GRUB usada, esperando arquivo de configuração do GRUB em um local diferente.</li><li>• Sistema de arquivos não compatível usado para armazenar seu arquivo de configuração de GRUB (por exemplo, convertendo o sistema de arquivos raiz a um tipo que não é compatível com uma versão anterior do GRUB).</li></ul>

## Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Opção 1: Modifique a AMI e reexecute a instância:</p> <ol style="list-style-type: none"><li>1. Modifique as AMIs de origem para criar um arquivo de configuração GRUB no local padrão (/boot/grub/menu.lst).</li><li>2. Verifique se sua versão do GRUB oferece suporte ao tipo de sistema de arquivos e atualize o GRUB, se necessário.</li><li>3. Escolha a imagem de GRUB adequada, (unidade hd0-1st ou hd00 – 1º unidade, 1ª partição).</li><li>4. Encerre a instância e execute uma nova usando a AMI criada.</li></ol> <p>Opção 2: Corrija a instância existente:</p> <ol style="list-style-type: none"><li>1. Pare a instância.</li><li>2. Separe o sistema de arquivos-raiz.</li><li>3. Associe o sistema de arquivos raiz para uma instância de trabalho conhecida.</li><li>4. Monte o sistema de arquivos.</li><li>5. Crie o arquivo de configuração do GRUB.</li><li>6. Verifique se sua versão do GRUB oferece suporte ao tipo de sistema de arquivos e atualize o GRUB, se necessário.</li><li>7. Separe o sistema de arquivos.</li><li>8. Associe à instância original.</li><li>9. Modifique o atributo do kernel para usar a imagem adequada do GRUB (1º disco ou 1ª partição no 1º disco).</li><li>10. Inicie a instância.</li></ol>
Com armazenamento de instâncias	<p>Opção 1: Modifique a AMI e reexecute a instância:</p> <ol style="list-style-type: none"><li>1. Crie a nova AMI com um arquivo de configuração GRUB no local padrão (/boot/grub/menu.lst).</li><li>2. Escolha a imagem de GRUB adequada, (unidade hd0-1st ou hd00 – 1º unidade, 1ª partição).</li><li>3. Verifique se sua versão do GRUB oferece suporte ao tipo de sistema de arquivos e atualize o GRUB, se necessário.</li><li>4. Encerre a instância e execute uma nova usando a AMI criada.</li></ol> <p>Opção 2: Encerre a instância e execute uma nova, especificando o kernel correto.</p>

Para este tipo de instância	Faça o seguinte
	<p>Note</p> <p>Para recuperar dados da instância existente, entre em contato com o <a href="#">AWS Support</a>.</p>

## Acessando a interface eth0: O dispositivo eth0 tem um endereço MAC diferente do esperado, ignorando. (Endereço MAC hard-coded)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
...
Bringing up loopback interface: [ OK ]
Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring.
[FAILED]
Starting auditd: [ OK ]
```

### Possíveis causas

Há uma interface MAC hard-coded na configuração da AMI

### Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Execute um destes procedimentos:</p> <ul style="list-style-type: none"><li>Modifique a AMI para remover o hard code e reexecute a instância.</li><li>Modifique a instância para remover o endereço MAC hard-coded.</li></ul> <p>OU</p> <p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>Pare a instância.</li><li>Separe o volume de raiz.</li><li>Associe o volume a outra instância e modifique o volume para remover o endereço MAC hard-coded.</li><li>Associe o volume à instância original.</li><li>Inicie a instância.</li></ol>
Com armazenamento de instâncias	Execute um destes procedimentos:

Para este tipo de instância	Faça o seguinte
	<ul style="list-style-type: none"><li>Modifique a instância para remover o endereço MAC hard-coded.</li><li>Encerre a instância e execute uma nova instância.</li></ul>

## Não foi possível carregar a Política do SELinux. A máquina está no modo de força. Parando agora. (Erro de configuração do SELinux)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

### Possíveis causas

O SELinux foi habilitado por engano:

- O kernel fornecido não é compatível com GRUB
- O kernel de fallback não existe

### Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"><li>Pare a instância com falha.</li><li>Separar o volume do dispositivo raiz da instância com falha.</li><li>Associe o volume do dispositivo raiz a outra instância do Linux em execução (posteriormente chamada de instância de recuperação).</li><li>Conecte-se à instância de recuperação e monte o volume do dispositivo raiz da instância falha.</li><li>Desabilite o SELinux no volume do dispositivo raiz montado. Esse processo varia nas distribuições de Linux; para obter mais informações, consulte a documentação específica do seu SO.</li></ol> <p>Note</p> <p>Em alguns sistemas, você desabilita o SELinux configurando SELINUX=disabled no arquivo <code>/mount_point/etc/sysconfig/</code></p>

Para este tipo de instância	Faça o seguinte
	<p><code>selinux</code>, onde <code>mount_point</code> é o local onde você montou o volume da sua instância de recuperação.</p> <p>6. Desmonte e separe o volume do dispositivo raiz da instância de recuperação e reassocie-o à instância original.</p> <p>7. Inicie a instância.</p>
Com armazenamento de instâncias	<p>Use o procedimento a seguir:</p> <ol style="list-style-type: none"> <li>1. Encerre a instância e execute uma nova instância.</li> <li>2. (Opcional) Procure assistência técnica para recuperação de dados usando o <a href="#">AWS Support</a>.</li> </ol>

## XENBUS: Excedido o limite de tempo para se conectar a dispositivos (tempo limite do Xenbus)

Essa condição é indicada por um log no sistema semelhante ao exibido abaixo.

```

Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found. Try passing init= option to kernel.
  
```

### Possíveis causas

- O dispositivo de blocos não está conectado à instância
- Essa instância está usando um kernel de uma instância antiga

### Ações sugeridas

Para este tipo de instância	Faça o seguinte
Baseado em Amazon EBS	<p>Execute um destes procedimentos:</p> <ul style="list-style-type: none"> <li>• Modifique a AMI e a instância para usar um kernel moderno e reexecutar a instância.</li> <li>• Reinicialize a instância.</li> </ul>
Com armazenamento de instâncias	<p>Execute um destes procedimentos:</p> <ul style="list-style-type: none"> <li>• Encerre a instância.</li> <li>• Modifique as AMIs para usar um kernel moderno e execute uma nova instância usando essa AMI.</li> </ul>

# Solucionar problemas de uma instância não acessível

É possível usar os seguintes métodos para solucionar problemas de uma instância do Linux não acessível. Para obter informações sobre solução de problemas de uma instância do Windows inacessível, consulte [Solucionar problemas de uma instância não acessível](#).

## Tópicos

- [Reinicialização da instância \(p. 1609\)](#)
- [Saída do console da instância \(p. 1609\)](#)
- [Fazer uma captura de tela de uma instância inacessível \(p. 1610\)](#)
- [Recuperação da instância quando um computador host falhar \(p. 1611\)](#)

## Reinicialização da instância

A capacidade de reiniciar instâncias que de outra forma seriam inacessíveis é valiosa para a solução de problemas e o gerenciamento geral de instâncias.

Assim como poderá redefinir um computador pressionando o botão de restauração, você pode também redefinir instâncias do EC2 usando o console, a CLI ou a API do Amazon EC2. Para obter mais informações, consulte [Reiniciar a instância \(p. 583\)](#)

### Warning

Para instâncias do Windows, essa operação executa um "hard reboot" que pode realizar a corrupção de dados.

## Saída do console da instância

A saída do console é uma ferramenta valiosa para o diagnóstico de problemas. É especialmente útil para resolver problemas de kernel e problemas de configuração de serviço que possam fazer com que uma instância seja encerrada ou torne-se inalcançável antes de seu daemon SSH ser iniciado.

Para o Linux/Unix, a saída do console da instância exibe a saída exata do console que normalmente seria exibida em um monitor físico associado a um computador. A saída do console retorna as informações armazenadas em buffer que foram postadas logo após um estado de transição de instância (iniciar, parar, reiniciar e finalizar). A saída publicada não é atualizada continuamente; somente quando for provável que seja do valor principal.

Para instâncias do Windows, a saída do console da instância inclui os últimos três erros do log de eventos do sistema.

É possível recuperar a saída mais recente do console de série em qualquer momento durante o ciclo de vida da instância. Essa opção só é compatível com [Instâncias criadas no Sistema Nitro \(p. 210\)](#). Não é compatível por meio do console do Amazon EC2.

### Note

Somente os 64 KB mais recentes da saída postada são armazenados, que estão disponíveis por no mínimo 1 hora após a última postagem.

Somente o proprietário da instância pode acessar a saída do console. Você pode recuperar a saída do console para suas instâncias usando o console ou a linha de comando.

Use um dos métodos a seguir para obter o resultado do console.

#### New console

##### Para obter o resultado do console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação à esquerda, escolha Instâncias e selecione a instância.
3. Escolha Actions (Ações), Monitor and troubleshoot (Monitorar e solucionar problemas), Get system log Obter log do sistema.

#### Old console

##### Para obter o resultado do console

1. Abra o console do Amazon EC2 em <https://console.aws.amazon.com/ec2/>.
2. No painel de navegação à esquerda, escolha Instâncias e selecione a instância.
3. Selecione Ações, Configurações da instância, Obter log do sistema.

#### Command line

##### Para obter o resultado do console

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

- [get-console-output](#) (AWS CLI)
- [Get-EC2ConsoleOutput](#) (AWS Tools for Windows PowerShell)

Para mais informações sobre erros comuns do log do sistema, consulte [Solução de problemas de erros de logs do sistema para instâncias baseadas em Linux \(p. 1588\)](#).

## Fazer uma captura de tela de uma instância inacessível

Se você não conseguir alcançar sua instância via SSH ou RDP, poderá fazer uma captura de tela da sua instância e vê-la como imagem. A imagem pode dar visibilidade quanto ao status da instância e permite uma solução de problemas mais rápida. Você pode gerar capturas de tela enquanto a instância estiver em execução ou após haver falha. Não há custo de transferência de dados custos para essa 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 \*.metal) ou é equipada com processadores Graviton ou Graviton 2 baseados em Arm. Este recurso está disponível nas seguintes regiões:

- US East (N. Virginia) Region
- US East (Ohio) Region
- US West (Oregon) Region
- US West (N. California) Region
- Europe (Ireland) Region
- Europe (Frankfurt) Region
- Asia Pacific (Tokyo) Region
- Asia Pacific (Seoul) Region
- Asia Pacific (Singapore) Region

- Asia Pacific (Sydney) Region
- South America (São Paulo) Region
- Asia Pacific (Mumbai) Region
- Canada (Central) Region
- Europe (London) Region
- Região Europa (Paris)

Para acessar o console da instância

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).
5. Selecione Get instance screenshot (Obter captura de tela da instância).

Clique com o botão direito sobre a imagem para fazer download dela e salvá-la.

Para fazer uma captura de tela usando a linha de comando

Você pode usar um dos comandos a seguir. O conteúdo apresentado 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)

## Recuperação da instância quando um computador host falhar

Se houver um problema irrecuperável com o hardware de um computador host subjacente, a AWS poderá programar um evento de interrupção da instância. Você será notificado desse evento com antecedência, por e-mail.

Para recuperar uma instância com Amazon EBS sendo executada em um computador host que falhou

1. Faça backup de todos os dados importantes nos volumes do seu armazenamento de instâncias para Amazon EBS ou Amazon S3.
2. Pare a instância.
3. Inicie a instância.
4. Restaure todos os dados importantes.

Para obter mais informações, consulte [Interromper e iniciar sua instância \(p. 562\)](#).

Para recuperar uma instância com armazenamento de instâncias executada em um computador host que falhou

1. Crie um AMI a partir da instância.
2. Faça upload da imagem para Amazon S3.
3. Faça backup dos dados importantes para Amazon EBS ou Amazon S3.
4. Encerre a instância.

5. Execute uma nova instância a partir da AMI.
6. Restaure todos os dados importantes para a nova instância.

Para obter mais informações, consulte [Criar uma AMI em Linux com armazenamento de instâncias \(p. 112\)](#).

## Inicialização a partir do volume errado

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.

Isso ocorre por conta de como funciona o ramdisk inicial no Linux. O volume definido como `/` em `/etc/fstab` é escolhido e, em algumas distribuições, isso é determinado pelo rótulo anexado à partição do volume. Mais especificamente, você descobrirá que seu `/etc/fstab` parece com o seguinte:

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Se você verificar os rótulos dos dois volumes, verá que ambos contêm o rótulo `/`:

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

Neste exemplo, pode acontecer de `/dev/xvdf1` acabar sendo o dispositivo raiz no qual sua instância se inicia após a execução inicial do ramdisk, em vez de o volume `/dev/xvda1` do qual você pretendeu inicializar. Para resolver isso, use o mesmo comando `e2label` para alterar o rótulo do volume associado do qual você não deseja inicializar.

Em alguns casos, especificar um UUID em `/etc/fstab` pode resolver isso. No entanto, se ambos os volumes vierem do mesmo snapshot ou o secundário for criado a partir de um snapshot do volume primário, eles compartilharão um UUID.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

Para alterar a identificação de um volume ext4 associado

1. Use o comando `e2label` para alterar a identificação do volume para outra coisa além de `/`.

```
[ec2-user ~]$ sudo e2label /dev/xvdf1 old/
```

2. Verifique se o volume tem a nova identificação.

```
[ec2-user ~]$ sudo e2label /dev/xvdf1
```

old/

Para alterar a identificação de um volume xfs associado

- Use o comando xfs\_admin para alterar a identificação do volume para outra coisa além de /.

```
[ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
writing all SBs
new label = "old/"
```

Depois de alterar a identificação do volume como mostrado, você poderá reiniciar a instância e selecionar o volume adequado pelo ramdisk inicial quando a instância for inicializada.

#### Important

Se você pretende desanexar o volume com o novo rótulo e devolvê-lo a outra instância para ser usado como o volume raiz, deverá executar novamente o procedimento acima e alterar o rótulo do volume de volta ao seu valor original. Caso contrário, a outra instância não é inicializada porque o disco ramdisk não consegue encontrar o volume com o rótulo /.

## Usar o EC2Rescue para Linux

O EC2Rescue para Linux é uma ferramenta de código aberto fácil de usar que pode ser executada na instância Linux do Amazon EC2 para diagnosticar e resolver problemas comuns usando sua biblioteca de mais de 100 módulos. Alguns casos de uso generalizados para o EC2Rescue para Linux incluem reunir syslog e logs do gerenciador de pacotes, coletar dados de utilização de recursos e diagnosticar/corrigir parâmetros problemáticos de kernel conhecidos e problemas comuns de OpenSSH.

O runbook [AWS Support-TroubleshootSSH](#) instala o EC2Rescue para Linux e, em seguida, usa a ferramenta para verificar ou tentar corrigir problemas comuns que impedem uma conexão remota a uma máquina Linux via SSH. Para obter mais informações e para executar essa automação, consulte [AWS Support-TroubleshootSSH](#).

Se você estiver usando uma instância Windows, consulte [EC2Rescue para Windows Server](#).

#### Contents

- [Instalar o EC2Rescue para Linux \(p. 1613\)](#)
- [Trabalhar com EC2Rescue para Linux \(p. 1617\)](#)
- [Desenvolver módulos do EC2Rescue \(p. 1619\)](#)

## Instalar o EC2Rescue para Linux

A ferramenta EC2Rescue para Linux pode ser instalada em uma instância Linux do Amazon EC2 que atenda aos seguintes pré-requisitos.

#### Prerequisites

- Sistemas operacionais com suporte:
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+

- RHEL 7+
- Ubuntu 16.04+
- Requisitos de software:
  - Python 2.7.9+ ou 3.2+

O runbook `AWSSupport-TroubleshootSSH` instala o EC2Rescue para Linux e, em seguida, usa a ferramenta para verificar ou tentar corrigir problemas comuns que impedem uma conexão remota a uma máquina Linux via SSH. Para obter mais informações e para executar essa automação, consulte [AWS Support-TroubleshootSSH](#).

Se o seu sistema tem a versão necessária do Python, você pode instalar a compilação padrão. Caso contrário, você pode instalar a compilação do pacote, incluindo uma cópia mínima do Python.

Para instalar a compilação padrão

1. Em uma instância Linux de trabalho, faça download da ferramenta [EC2Rescue para Linux](#):

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
```

2. (Opcional) Antes de continuar, você também pode verificar a assinatura do arquivo de instalação do EC2Rescue para Linux. Para obter mais informações, consulte [\(Opcional\) Verifique a assinatura de EC2Rescue para Linux \(p. 1614\)](#).
3. Faça download do arquivo hash sha256:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
```

4. Verifique a integridade do tarball:

```
sha256sum -c ec2rl.tgz.sha256
```

5. Desembale o tarball:

```
tar -xzvf ec2rl.tgz
```

6. Verifique instalação listando o arquivo de ajuda:

```
cd ec2rl-<version_number>
./ec2rl help
```

Para instalar a compilação do pacote

Para obter um link para download e uma lista de limitações, consulte [EC2Rescue para Linux](#) no GitHub.

## (Opcional) Verifique a assinatura de EC2Rescue para Linux

Veja a seguir o processo recomendado para verificação da validade do pacote do EC2Rescue para Linux para sistemas operacionais Linux.

Sempre que baixar um aplicativo da Internet, recomendamos que você autentique a identidade do fornecedor do software e verifique se o aplicativo não foi alterado ou corrompido desde que foi publicado. Isso protege você contra a instalação de uma versão do aplicativo que contenha um vírus ou outro código mal-intencionado.

Se depois de executar as etapas neste tópico, você determinar que o software do EC2Rescue para Linux está alterado ou corrompido, não execute o arquivo de instalação. Em vez disso, entre em contato com o Amazon Web Services.

Os arquivos do EC2Rescue para Linux para os sistemas operacionais baseados em Linux são assinados usando o GnuPG, uma implementação de código aberto do padrão OpenPGP (Pretty Good Privacy) para assinaturas digitais seguras. O GnuPG (também conhecido como GPG) fornece autenticação e verificação de integridade por meio de uma assinatura digital. A AWS publica uma chave pública e assinaturas que você pode usar para verificar o pacote EC2Rescue para Linux que foi obtido por download. Para obter mais informações sobre o PGP e o GnuPG (GPG), consulte <http://www.gnupg.org>.

A primeira etapa é estabelecer confiança com o fornecedor do software. Faça download da chave pública do fornecedor do software, verifique se o proprietário da chave pública é quem afirma ser e, em seguida, adicione a chave pública ao seu keyring. O keyring é um conjunto de chaves públicas conhecidas. Após estabelecer a autenticidade da chave pública, você pode usá-la para verificar a assinatura do aplicativo.

#### Tarefas

- [Instalar as ferramentas do GPG \(p. 1615\)](#)
- [Autenticar e importar a chave pública \(p. 1615\)](#)
- [Verificar a assinatura do pacote \(p. 1616\)](#)

## Instalar as ferramentas do GPG

Se o seu sistema operacional for Linux ou Unix, as ferramentas do GPG já poderão estar instaladas. Para testar se as ferramentas estão instaladas no sistema, digite gpg2 em um prompt de comando. Se as ferramentas do GPG estiverem instaladas, um prompt de comando do GPG será exibido. Se as ferramentas do GPG não estiverem instaladas, uma mensagem de erro será exibida informando que o comando não pode ser encontrado. Você pode instalar o pacote GnuPG a partir de um repositório.

Para instalar as ferramentas do GPG no Linux baseado em Debian

- Em um terminal, execute o comando a seguir:

```
apt-get install gnupg2
```

Para instalar as ferramentas do GPG no Linux baseado em Red Hat

- Em um terminal, execute o comando a seguir:

```
yum install gnupg2
```

## Autenticar e importar a chave pública

A próxima etapa do processo é autenticar a chave pública do EC2Rescue para Linux e adicioná-la como uma chave confiável ao seu keyring do GPG.

Para autenticar e importar a chave pública do EC2Rescue para Linux

1. Em um aviso de comando, use o seguinte comando para obter uma cópia de nossa chave de compilação de público GPG:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
```

2. Em um prompt de comando no diretório onde você salvou `ec2rl.key`, use o comando a seguir para importar a chave pública do EC2Rescue para Linux para seu keyring:

```
gpg2 --import ec2rl.key
```

O comando retorna resultados semelhantes a:

```
gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>" imported
gpg: Total number processed: 1
gpg:          imported: 1  (RSA: 1)
```

## Verificar a assinatura do pacote

Depois de instalar as ferramentas do GPG, autenticar e importar a chave pública do EC2Rescue para Linux e verificar se a chave pública do EC2Rescue para Linux é confiável, você estará pronto para verificar a assinatura do script de instalação do EC2Rescue para Linux.

Para verificar o script de instalação da assinatura do EC2Rescue para Linux

1. Em um prompt de comando, execute o comando a seguir para baixar o arquivo de assinatura para o script de instalação:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
```

2. Verifique a assinatura executando o comando a seguir em um prompt no diretório onde você salvou o `ec2rl.tgz.sig` e o arquivo de instalação EC2Rescue para Linux. Ambos os arquivos devem estar presentes.

```
gpg2 --verify ./ec2rl.tgz.sig
```

A saída deve parecer com algo semelhante ao seguinte:

```
gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C C36A F780 4843 2FAE 2A1C
Subkey fingerprint: 966B 0D27 85E9 AEEC 1146 7A9D 8851 1153 6991 ED45
```

Se a saída contém a frase `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"`, isso significa que a assinatura foi confirmada com êxito e você pode dar continuidade à execução do script de instalação do EC2Rescue para Linux.

Se a saída inclui a frase `BAD signature`, verifique se você executou o procedimento corretamente. Se você continuar a receber essa resposta, entre em contato com o Amazon Web Services e não execute o arquivo de instalação que baixou anteriormente.

Veja a seguir os detalhes sobre as advertências que talvez sejam exibidas:

- **WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner.** Isso se refere ao seu nível pessoal de confiança de que você tem uma chave pública autêntica para o EC2Rescue para Linux. A situação ideal seria você visitar um escritório do

Amazon Web Services e receber uma chave em pessoa. No entanto, é mais frequente você baixá-la de um site. Nesse caso, o site é um Amazon Web Services.

- gpg2: no ultimately trusted keys found. Isso significa que a chave específica não é "essencialmente confiável" (por você ou por outras pessoas que você confia).

Para obter mais informações, consulte <http://www.gnupg.org>.

## Trabalhar com EC2Rescue para Linux

Veja a seguir as tarefas comuns que você pode realizar para começar a usar essa ferramenta.

### Tarefas

- [Executar EC2Rescue para Linux \(p. 1617\)](#)
- [Fazer upload dos resultados \(p. 1618\)](#)
- [Criar backups \(p. 1618\)](#)
- [Obter ajuda \(p. 1618\)](#)

## Executar EC2Rescue para Linux

Você pode executar o EC2Rescue para Linux conforme mostrado nos exemplos a seguir.

Example Exemplo: executar todos os módulos

Para executar todos os módulos, execute o EC2Rescue para Linux sem opções:

```
./ec2rl run
```

Alguns módulos exigem o acesso raiz. Se você não é um usuário raiz, use o comando sudo para executar esses módulos da seguinte maneira:

```
sudo ./ec2rl run
```

Example Exemplo: executar um módulo específico

Para executar apenas módulos específicos, use o parâmetro --only-modules:

```
./ec2rl run --only-modules=module_name --arguments
```

Por exemplo, este comando executa o módulo dig para consultar o domínio amazon.com:

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Example Exemplo: visualizar os resultados

Você pode visualizar os resultados em /var/tmp/ec2rl:

```
cat /var/tmp/ec2rl/logfile_location
```

Por exemplo, visualize o arquivo de log para o módulo dig:

```
cat /var/tmp/ec2rl/2017-05-11T15_39_21.893145/mod_out/run/dig.log
```

## Fazer upload dos resultados

Se o AWS Support solicitou os resultados, ou para compartilhar os resultados de um bucket do S3, carregue-os usando a ferramenta da CLI EC2Rescue para Linux. A saída dos comandos do EC2Rescue para Linux devem fornecer os comandos que você precisa usar.

Example Exemplo: Carregar resultados para AWS Support

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --support-url="URLProvidedByAWSupport"
```

Example Exemplo: carregar os resultados em um bucket do S3

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --presigned-url="YourPresignedS3URL"
```

Para obter mais informações sobre como gerar pre-signed URLs para o Amazon S3, consulte [Fazer upload de objetos usando pre-signed URLs](#).

## Criar backups

Crie um backup para sua instância, um ou mais volumes, ou um ID de dispositivo específico usando os seguintes comandos.

Example Exemplo: fazer backup de uma instância usando uma imagem de máquina da Amazon (AMI)

```
./ec2rl run --backup=ami
```

Example Exemplo: fazer backup de todos os volumes associados à instância

```
./ec2rl run --backup=allvolumes
```

Example Exemplo: fazer backup de um volume específico

```
./ec2rl run --backup=volumeID
```

## Obter ajuda

O EC2Rescue para Linux inclui um arquivo de ajuda que fornece informações e a sintaxe para cada comando disponível.

Example Exemplo: exibir a ajuda geral

```
./ec2rl help
```

Example Exemplo: listar os módulos disponíveis

```
./ec2rl list
```

Example Exemplo: exibir a ajuda para um módulo específico

```
./ec2rl help module_name
```

Por exemplo, use o comando a seguir para mostrar o arquivo de ajuda do módulo dig:

```
./ec2rl help dig
```

## Desenvolver módulos do EC2Rescue

Os módulos são gravados em YAML, um padrão de serialização de dados. O arquivo YAML de um módulo consiste em um único documento, representando o módulo e seus atributos.

### Adicionar atributos de módulo

A tabela a seguir lista os atributos de módulo disponíveis.

Atributo	Descrição
name	O nome do módulo. O nome precisa ter 18 caracteres ou menos.
versão	O número da versão do módulo.
title	Um título curto e descritivo para o módulo. Esse valor precisa ter 50 caracteres ou menos.
helptext	A descrição estendida do módulo. Cada linha precisa ter 75 caracteres ou menos. Se o módulo utilizar argumentos, obrigatórios ou opcionais, inclua-os no valor helptext.  Por exemplo: <pre>helptext: !!str     Collect output from ps for system   analysis   Consumes --times= for number of times to   repeat   Consumes --period= for time period   between repetition</pre>
posicionamento	O estágio no qual o módulo deve ser executado. Valores com suporte: <ul style="list-style-type: none"><li>pré-diagnóstico</li><li>executar</li><li>pós-diagnóstico</li></ul>
linguagem	A linguagem em que o código do módulo está escrito. Valores com suporte: <ul style="list-style-type: none"><li>bash</li><li>python</li></ul> <p>Note</p> <p>O código Python deve ser compatível com o Python 2.7.9+ e o Python 3.2+.</p>

Atributo	Descrição
correção	Indica se o módulo dá suporte a correção. Os valores compatíveis são <code>True</code> ou <code>False</code> .  Os padrões do módulo de <code>False</code> se estiver ausente, tornando-o um atributo opcional para esses módulos que não dão suporte a correção.
conteúdo	A totalidade do código do script.
restrição	O nome do objeto que contém os valores de limite.
domínio	Um descritor de como o módulo é agrupado ou classificado. O conjunto de módulos incluídos usa os seguintes domínios: <ul style="list-style-type: none"><li>• aplicativo</li><li>• net</li><li>• os</li><li>• desempenho</li></ul>
classe	Um descritor do tipo da tarefa executada pelo módulo. O conjunto de módulos incluídos usa as seguintes classes: <ul style="list-style-type: none"><li>• coletar (coleta a saída dos programas)</li><li>• diagnosticar (é aprovado/falha com base em um conjunto de critérios)</li><li>• recolher (copia os arquivos e grava em um arquivo específico)</li></ul>
distro	A lista de distribuições Linux às quais esse módulo oferece suporte. O conjunto de módulos usa as seguintes distribuições: <ul style="list-style-type: none"><li>• alami (Amazon Linux)</li><li>• rhel</li><li>• ubuntu</li><li>• suse</li></ul>
obrigatório	Os argumentos necessários que o módulo está consumindo das opções de CLI.
opcional	Os argumentos opcionais que o módulo pode usar.
software	Os executáveis de software usados no módulo. Esse atributo deve especificar o software que não é instalado por padrão. A lógica do EC2Rescue para Linux garante que esses programas estejam presentes e executáveis antes de executar o módulo.

Atributo	Descrição
pacote	O pacote de software de origem para um executável. Esse atributo deve fornecer detalhes estendidos sobre o pacote com o software, incluindo uma URL para fazer download ou obter mais informações.
sudo	Indica se o acesso raiz é necessário para executar o módulo.  Não é necessário implementar verificações sudo no script do módulo. Se o valor for verdadeiro, a lógica do EC2Rescue para Linux só executará o módulo quando o usuário que estiver executando tiver acesso raiz.
perfimpact	Indica se o módulo pode ter impacto significativo no desempenho no ambiente no qual ele está sendo execução. Se o valor for verdadeiro e o argumento --perfimpact=true não estiver presente, o módulo será ignorado.
parallelexclusive	Especifica um programa que exija exclusividade mútua. Por exemplo, todos os módulos que especificam "bpf" executados de maneira serial.

## Adicionar variáveis de ambiente

A tabela a seguir lista as variáveis de ambiente disponíveis.

Variável de ambiente	Descrição
<code>EC2RL_CALLPATH</code>	O caminho para <code>ec2rl.py</code> . Esse caminho pode ser usado para encontrar o diretório lib e utilizar os módulos Python do fornecedor.
<code>EC2RL_WORKDIR</code>	O diretório tmp principal para a ferramenta de diagnóstico.  Valor padrão: <code>/var/tmp/ec2rl</code> .
<code>EC2RL_RUNDIR</code>	O diretório no qual a saída é armazenada.  Valor padrão: <code>/var/tmp/ec2rl/&lt;date&amp;timestamp&gt;</code> .
<code>EC2RL_GATHEREDDIR</code>	O diretório raiz para colocar os dados de módulo reunidos.  Valor padrão: <code>/var/tmp/ec2rl/&lt;date&amp;timestamp&gt;/mod_out/gathered/</code> .
<code>EC2RL_NET_DRIVER</code>	O driver em uso na primeira interface de rede não virtual, ordenada alfabeticamente, na instância.  Exemplos:

Variável de ambiente	Descrição
	<ul style="list-style-type: none"><li>• xen_netfront</li><li>• ixgbevf</li><li>• ena</li></ul>
EC2RL_SUDO	Verdadeiro se EC2Rescue para Linux estiver em execução como raiz; caso contrário, falso.
EC2RL_VIRT_TYPE	O tipo de virtualização conforme fornecido pelos metadados da instância.  Exemplos: <ul style="list-style-type: none"><li>• default-hvm</li><li>• default-paravirtual</li></ul>
EC2RL_INTERFACES	Uma lista enumerada de interfaces no sistema. O valor é uma string que contém nomes, como eth0eth1, etc. É gerada pelo <code>functions.bash</code> e está disponível somente para os módulos que a originaram.

## Usar sintaxe de YAML

Os seguintes itens devem ser observados ao construir os arquivos YAML do módulo:

- O hífen triplo (---) denota o início explícito de um documento.
- A tag `!ec2rlcore.module.Module` indica para o analisador YAML qual construtor chamar ao criar o objeto do fluxo de dados. Você pode localizar o construtor no arquivo `module.py`.
- A tag `!!str` diz para o analisador YAML não tentar determinar o tipo de dados e, em vez disso, interpretar o conteúdo como um literal de string.
- O caractere pipe (|) informa ao analisador YAML que o valor é um escalar de estilo literal. Nesse caso, o analisador inclui todos os espaços em branco. É importante para os módulos porque o recuo e os caracteres de nova linha são mantidos.
- O recuo padrão YAML é dois espaços, que podem ser vistos nos exemplos a seguir. Certifique-se de manter o recuo padrão (por exemplo, quatro espaços para Python) para o script e, em seguida, defina o recuo de dois espaços para todo o conteúdo no arquivo do módulo.

## Exemplos de módulos

Exemplo 1 (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
    Collect output from ps for system analysis
    Requires --times= for number of times to repeat
    Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
```

```
language: !!str bash
content: !!str |
#!/bin/bash
error_trap()
{
    printf "%0.s=" {1..80}
    echo -e "\nERROR: \"$BASH_COMMAND\" exited with an error on line ${BASH_LINENO[0]}"
    exit 0
}
trap error_trap ERR

# read-in shared function
source functions.bash
echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every $period
seconds."
for i in $(seq 1 $times); do
    ps auxww
    sleep $period
done
constraint:
requires_ec2: !!str False
domain: !!str performance
class: !!str collect
distro: !!str alami ubuntu rhel suse
required: !!str period times
optional: !!str
software: !!str
sudo: !!str False
perfimpact: !!str False
parallelexclusive: !!str
```

## EC2 Serial Console para instâncias do Linux

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 \(p. 1624\)](#).

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 Windows, consulte [Console serial do EC2 para instâncias do Windows](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

### Tópicos

- [Configurar o acesso ao console serial do EC2 \(p. 1624\)](#)
- [Conectar-se ao console serial do EC2 \(p. 1629\)](#)
- [Encerrar uma sessão do console serial do EC2 \(p. 1634\)](#)

- Solucionar problemas da instância do Linux usando o EC2 Serial Console (p. 1635)

## 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. Você também deve configurar um usuário com senha em cada instância para que seus usuários possam usar o console serial para solução de problemas.

### Tópicos

- [Níveis de acesso ao console serial do EC2 \(p. 1624\)](#)
- [Gerenciar o acesso da conta ao console serial do EC2 \(p. 1624\)](#)
- [Configurar políticas do IAM para acesso ao console serial do EC2 \(p. 1627\)](#)
- [Definir uma senha de usuário do SO \(p. 1628\)](#)

## 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 \(p. 1624\)](#).

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 \(p. 1627\)](#).

### 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 \(p. 1627\)](#).

### Nível do SO

Você pode definir uma senha de usuário no nível do SO convidado. Isso fornece acesso ao console serial para alguns casos de uso. No entanto, para monitorar os logs, você não precisa de um usuário com senha. Para obter mais informações, consulte [Definir uma senha de usuário do SO \(p. 1628\)](#).

## 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 \(p. 1625\)](#)
- [Exibir status de acesso da conta no console serial \(p. 1625\)](#)
- [Conceder acesso da conta ao console serial \(p. 1626\)](#)
- [Negar acesso da conta ao console serial \(p. 1626\)](#)

## 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.

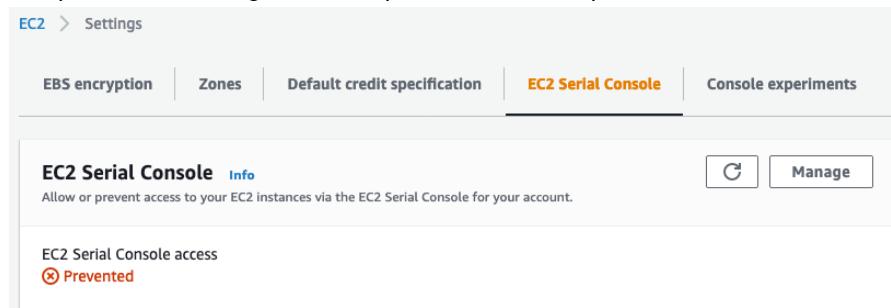
## Exibir status de acesso da conta no console serial

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:SendSerialConsoleSSHPublicKey`. 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 \(p. 1627\)](#)
- [Explicitamente negar acesso ao console serial \(p. 1627\)](#)
- [Usar tags de recursos para controlar o acesso ao console serial \(p. 1628\)](#)

### 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:SendSerialConsoleSSHPublicKey"  
            ],  
            "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}"  
                }  
            }  
        ]  
    }  
}
```

## Definir uma senha de usuário do SO

Você pode se conectar ao console serial sem uma senha. No entanto, para usar o console serial para solucionar problemas de uma instância, a instância deve ter um usuário com senha.

Você pode definir a senha para qualquer usuário do sistema operacional, incluindo o usuário raiz. Observe que o usuário raiz pode modificar todos os arquivos, enquanto cada usuário do sistema operacional pode ter permissões limitadas.

Você deve definir uma senha de usuário para cada instância para a qual você usará o console serial. Essa é uma exigência única de cada instância.

Note

As instruções a seguir só são aplicáveis se você tiver executado sua instância usando uma AMI fornecida pela AWS porque, por padrão, as AMIs fornecidas pela AWS não são configuradas com um usuário com senha. Se você tiver executado a instância usando uma AMI que já tenha a senha do usuário raiz configurada, poderá ignorar essas instruções.

Para definir uma senha do usuário

1. [Connect \(p. 535\) \(Conectar\) \(Conecte-se\)](#) à instância. Você pode usar qualquer método para se conectar à instância, exceto o método de conexão do console serial do EC2.
2. Para definir a senha para um usuário, use o comando `passwd`. No exemplo a seguir, o usuário é `root`.

```
[ec2-user ~]$ sudo passwd root
```

A seguir está um exemplo de saída.

```
Changing password for user root.  
New password:
```

3. No prompt `New password`, digite a nova senha.
4. No prompt, digite novamente a senha.

## 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 Linux usando o EC2 Serial Console \(p. 1635\)](#).

Tópicos

- [Considerations \(p. 1629\)](#)
- [Prerequisites \(p. 1630\)](#)
- [Conectar-se ao console serial do EC2 \(p. 1630\)](#)
- [Impressões digitais do console serial EC2 \(p. 1633\)](#)

## 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 Linux: `ttyS0`
- 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 \(p. 1624\)](#).
  - [Configurar políticas do IAM para acesso ao console serial do EC2 \(p. 1627\)](#) Todos os usuários do IAM que usarão o console serial devem ter as permissões necessárias.
  - [Definir uma senha de usuário do SO \(p. 1628\)](#).
- Para se conectar ao console serial [Usando o cliente com base em navegador \(p. 1630\)](#), seu navegador deve suportar WebSocket. Se o navegador não suportar WebSocket, conecte-se ao console serial [Usando sua própria chave e um cliente SSH. \(p. 1631\)](#)
- 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 \(p. 503\)](#).
- 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 \(p. 1630\)](#)
- [Conectar-se usando sua própria chave e cliente SSH \(p. 1631\)](#)

### 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 \(p. 1624\)](#).
- Use o SysRq para se conectar ao console serial. O SysRq não exige que você se conecte por meio do cliente com base em navegador. Para obter mais informações, consulte [Solucionar problemas de instâncias do Linux usando SysRq \(p. 1638\)](#).
- Reinicie o getty. Se você tiver acesso SSH à instância, conecte-se à instância usando SSH e reinicie o getty usando o comando a seguir.

```
[ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
```

- Reinicie a instância. Você pode reiniciar sua instância usando o SysRq, o console do EC2 ou a AWS CLI. Para obter mais informações, consulte [Solucionar problemas de instâncias do Linux usando SysRq \(p. 1638\)](#) ou [Reiniciar a instância \(p. 583\)](#).

5. No prompt `login`, insira o nome do usuário com senha que você [configurou anteriormente \(p. 1628\)](#) e, a seguir, pressione Enter.
6. No prompt `Password`, insira a senha e, a seguir, pressione Enter.

Agora, você está conectado à instância e pode usar o console serial para solucionar problemas.

## 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.

```
$ 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`.

```
$ 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`.

```
$ 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 \(p. 1633\)](#).

```
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 \(p. 1624\)](#).
- Use o SysRq para se conectar ao console serial. O SysRq não exige que você se conecte via SSH. Para obter mais informações, consulte [Solucionar problemas de instâncias do Linux usando SysRq \(p. 1638\)](#).
- Reinicie o getty. Se você tiver acesso SSH à instância, conecte-se à instância usando SSH e reinicie o getty usando o comando a seguir.

```
[ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
```

- Reinicie a instância. Você pode reiniciar sua instância usando o SysRq, o console do EC2 ou a AWS CLI. Para obter mais informações, consulte [Solucionar problemas de instâncias do Linux usando SysRq \(p. 1638\)](#) ou [Reiniciar a instância \(p. 583\)](#).
- 5. No prompt **Login**, insira o nome do usuário com senha que você [configurou anteriormente \(p. 1628\)](#)e, a seguir, pressione Enter.
- 6. No prompt **Password**, insira a senha e, a seguir, pressione Enter.

Agora, você está conectado à instância e pode usar o console serial para solucionar problemas.

## 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:EhwPkTzRtTY7TRSzz6XbB0/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/O8TUX7LQgZuaC6L45CoY
```

- ap-southeast-2 – Ásia-Pacífico (Sydney)

```
SHA256:yFvMwUK91EUQjQTRoXXzuN+cW9/VSe9W984Cf5Tgzo4
```

- ap-northeast-1 – Ásia-Pacífico (Tóquio)

```
SHA256:RQfsDCZTOfQawewTRDV1t9Em/HMrFQe+CR1IOT5um4k
```

- ca-central-1: Canadá (Central)

```
SHA256:P202jOZwmpMwkp06YW738FIOTHdUTyEv2gczYMM07s4
```

- eu-central-1 – Europa (Frankfurt)

```
SHA256:aCMFS/yIcOd0lkXv018AmZ1Toe+bBnrJJ3Fy0k0De2c
```

- eu-west-1 – Europa (Irlanda)

```
SHA256:h2AaGAWO4Hathhtm6ezs3Bj7udgUxi2qTrHjZAwCW6E
```

- eu-west-2: Europa (Londres)

```
SHA256:a69rd5CE/AEG4Amm53I6lkD1ZPvS/BCV3tTPW2RnJg8
```

- eu-west-3: Europa (Paris)

```
SHA256:q81dnAf9pymeNe8BnFVngY3RPAr/kxswJUzfrlxeeEWs
```

- eu-north-1: Europa (Estocolmo)

```
SHA256:tkGFFUVUDvocDiGSS3Cu8Gdl6w2uI32EPNpKFKLwX84
```

- sa-east-1: América do Sul (São Paulo)

```
SHA256:rd2+/320gnjewlyVIemENaQzC+Botbih620qAPDq1dI
```

- us-gov-east-1: AWS GovCloud (Leste dos EUA)

```
SHA256:tIwe19GWsoyLClrtvu38YEEh+DHIkqnDcZnmtebvF28
```

- us-gov-west-1: AWS GovCloud (Oeste dos EUA)

```
SHA256:kfOFRWLaoZfB+utbd3bRf80lPf8nGO2YZLqXZiIw5DQ
```

## 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.

```
$ ~.
```

### 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 Linux 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

- [Solucionar problemas de instâncias do Linux usando o GRUB \(p. 1635\)](#)
- [Solucionar problemas de instâncias do Linux usando SysRq \(p. 1638\)](#)

Para obter informações sobre como solucionar problemas de instâncias do Windows, consulte [Solucionar problemas de instâncias do Windows usando o console serial do EC2](#) no Guia do usuário do Amazon EC2 para instâncias do Windows.

## Solucionar problemas de instâncias do Linux usando o GRUB

O GNU GRUB (abreviatura de GNU GRand Unified Bootloader) é o carregador de inicialização padrão para a maioria dos sistemas operacionais Linux. No menu do GRUB, você pode selecionar em qual kernel inicializar ou modificar entradas de menu para alterar a forma como o kernel irá inicializar. Isso pode ser útil ao solucionar problemas de uma instância com falha.

O menu do GRUB é exibido durante o processo de inicialização. O menu não é acessível via SSH normal, mas você pode acessá-lo por meio do console serial do EC2.

### Tópicos

- [Prerequisites \(p. 1635\)](#)
- [Configurar o GRUB \(p. 1635\)](#)
- [Usar o GRUB \(p. 1637\)](#)

## Prerequisites

Antes de configurar e usar o GRUB, você deve conceder acesso ao console serial. Para obter mais informações, consulte [Configurar o acesso ao console serial do EC2 \(p. 1624\)](#).

## Configurar o GRUB

Antes de usar o GRUB por meio do console serial, você deve configurar a instância para usar o GRUB por meio do console serial.

Para configurar o GRUB, escolha um dos seguintes procedimentos com base na AMI que foi usada para executar a instância.

### Amazon Linux 2

Para configurar o GRUB em uma instância do Amazon Linux 2

1. [Conecte-se à sua instância \(p. 535\)](#).
2. Adicione ou altere as seguintes opções em `/etc/default/grub`:
  - Defina `GRUB_TIMEOUT=1`.
  - Adicionar `GRUB_TERMINAL="console serial"`.
  - Adicionar `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

Veja a seguir um exemplo de /etc/default/grub. Você pode precisar alterar a configuração com base na configuração do seu sistema.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0  
biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"  
GRUB_TIMEOUT=1  
GRUB_DISABLE_RECOVERY="true"  
GRUB_TERMINAL="console serial"  
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Aplique a configuração atualizada executando o comando a seguir.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

## Ubuntu

Para configurar o GRUB em uma instância do Ubuntu

1. [Conecte-se à sua instância \(p. 535\)](#).
2. Adicione ou altere as seguintes opções em /etc/default/grub.d/50-cloudimg-settings.cfg:
  - Defina GRUB\_TIMEOUT=1.
  - Adicionar GRUB\_TIMEOUT\_STYLE=menu.
  - Adicionar GRUB\_TERMINAL="console serial".
  - Remover GRUB\_HIDDEN\_TIMEOUT.
  - Adicionar GRUB\_SERIAL\_COMMAND="serial --speed=115200".

Veja a seguir um exemplo de /etc/default/grub.d/50-cloudimg-settings.cfg. Você pode precisar alterar a configuração com base na configuração do seu sistema.

```
# Cloud Image specific Grub settings for Generic Cloud Images  
# CLOUD_IMG: This file was created/modified by the Cloud Image build process  
  
# Set the recordfail timeout  
GRUB_RECORDFAIL_TIMEOUT=0  
  
# Do not wait on grub prompt  
GRUB_TIMEOUT=1  
GRUB_TIMEOUT_STYLE=menu  
  
# Set the default commandline  
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0  
nvme_core.io_timeout=4294967295"  
  
# Set the grub console type  
GRUB_TERMINAL="console serial"  
GRUB_SERIAL_COMMAND="serial --speed 115200"
```

3. Aplique a configuração atualizada executando o comando a seguir.

```
[ec2-user ~]$ sudo update-grub
```

---

RHEL

Para configurar o GRUB em uma instância do RHEL

1. [Conecte-se à sua instância \(p. 535\)](#).
2. Adicione ou altere as seguintes opções em `/etc/default/grub`:
  - Remover `GRUB_TERMINAL_OUTPUT`.
  - Adicionar `GRUB_TERMINAL="console serial"`.
  - Adicionar `GRUB_SERIAL_COMMAND="serial --speed=115200"`.

Veja a seguir um exemplo de `/etc/default/grub`. Você pode precisar alterar a configuração com base na configuração do seu sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_CMDLINE_LINUX="console=ttyS0,115200n8 console=tty0 net.ifnames=0
    rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
GRUB_DISABLE_RECOVERY="true"
GRUB_ENABLE_BLSCFG=true
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=115200"
```

3. Aplique a configuração atualizada executando o comando a seguir.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

CentOS

Para instâncias executadas usando uma AMI do CentOS, o GRUB é configurado para o console serial por padrão.

Veja a seguir um exemplo de `/etc/default/grub`. Sua configuração pode ser diferente com base na configuração do sistema.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
GRUB_DISABLE_RECOVERY="true"
```

## Usar o GRUB

Depois que o GRUB estiver configurado, conecte-se ao console serial e reinicie a instância com o comando de reinicialização. Durante a reinicialização, você verá o menu do GRUB. Pressione qualquer tecla quando o menu do GRUB aparecer para interromper o processo de inicialização, permitindo que você interaja com o menu do GRUB.

### Tópicos

- [Modo de usuário único \(p. 1638\)](#)
- [Modo de emergência \(p. 1638\)](#)

## Modo de usuário único

O modo de usuário único inicializará o kernel em um nível de execução inferior. Por exemplo, ele pode montar o sistema de arquivos, mas não ativar a rede, dando a você a oportunidade de realizar a manutenção necessária para corrigir a instância.

Para inicializar no modo de usuário único

1. [Connect \(p. 1630\)](#) (Conecte-se) ao console serial da instância.
2. Execute a instância usando o seguinte comando.

```
[ec2-user ~]$ sudo reboot
```

3. Durante a reinicialização, quando o menu do GRUB aparecer, pressione qualquer tecla para interromper o processo de inicialização.
4. No menu do GRUB, use as teclas de seta para selecionar o kernel para inicializar e pressione e no teclado.
5. Use as teclas de seta para posicionar o cursor na linha que contém o kernel. A linha começa com um `linux` ou `linux16`, dependendo da AMI usada para executar a instância. Para o Ubuntu, duas linhas começam com `linux`, que devem ser modificadas na próxima etapa.
6. No final da linha, adicione a palavra `single`.

Veja um exemplo a seguir para Amazon Linux 2.

```
linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
dadd-4499-938d-ebbf42c3e499 ro console=tty0 console=ttyS0,115200n8 net.ifname\
s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
ll=0 single
```

7. Pressione Ctrl+X para inicializar no modo de usuário único.
8. No prompt `login`, insira o nome do usuário com senha que você [configurou anteriormente \(p. 1628\)](#), e, a seguir, pressione Enter.
9. No prompt `Password`, insira a senha e, a seguir, pressione Enter.

## Modo de emergência

O modo de emergência é semelhante ao modo de usuário único, exceto que o kernel é executado no nível de execução mais baixo possível.

Para inicializar no modo de emergência, siga as etapas em [Modo de usuário único \(p. 1638\)](#) na seção anterior, mas, na etapa 6, adicione a palavra `emergency` em vez de `single`.

## Solucionar problemas de instâncias do Linux usando SysRq

A chave System Request (SysRq), que, às vezes, é denominada “SysRq mágica”, pode ser usada para enviar diretamente ao kernel um comando, fora de um shell, e o kernel responderá, independentemente do que o kernel está fazendo. Por exemplo, se a instância tiver parado de responder, você poderá usar a chave SysRq para dizer ao kernel para falhar ou reiniciar. Para obter mais informações, consulte [Chave SysRq mágica](#) na Wikipédia.

### Tópicos

- [Prerequisites \(p. 1639\)](#)
- [Configurar o SysRq \(p. 1639\)](#)
- [Usar o SysRq \(p. 1639\)](#)

## Prerequisites

Antes de configurar e usar o SysRq, você deve conceder acesso ao console serial. Para obter mais informações, consulte [Configurar o acesso ao console serial do EC2 \(p. 1624\)](#).

## Configurar o SysRq

Para configurar o SysRq, habilite os comandos do SysRq para o ciclo de inicialização atual. Para tornar a configuração persistente, você também pode habilitar os comandos SysRq para inicializações subsequentes.

Para habilitar todos os comandos SysRq para o ciclo de inicialização atual

1. [Conecte-se à sua instância \(p. 535\)](#).
2. Execute o seguinte comando.

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

### Note

Essa configuração será limpa na próxima reinicialização.

Para habilitar todos os comandos do SysRq para inicializações subsequentes

1. Crie o arquivo `/etc/sysctl.d/99-sysrq.conf` e abra-o no seu editor favorito.

```
[ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
```

2. Adicione a seguinte linha.

```
kernel.sysrq=1
```

3. Reinicie a instância para aplicar as alterações.

```
[ec2-user ~]$ sudo reboot
```

4. No prompt `login`, insira o nome do usuário com senha que você [configurou anteriormente \(p. 1628\)](#) e, a seguir, pressione Enter.
5. No prompt `Password`, insira a senha e, a seguir, pressione Enter.

## Usar o SysRq

Você pode usar comandos SysRq no cliente com base em navegador do console serial do EC2 ou em um cliente SSH. O comando que enviará uma solicitação de interrupção é diferente para cada cliente.

Para usar o SysRq, escolha um dos seguintes procedimentos com base no cliente que você está usando.

### Browser-based client

Para usar o SysRq no cliente com base em navegador do console serial

1. [Connect \(p. 1630\)](#) (Conecte-se) ao console serial da instância.
2. Para enviar uma solicitação de interrupção, pressione `CTRL+0` (zero). Se o teclado suportá-la, você também poderá enviar uma solicitação de interrupção usando a tecla `Pause` ou `Break`.

```
[ec2-user ~]$ CTRL+D
```

3. Para emitir um comando do SysRq, pressione a tecla no teclado que corresponde ao comando requerido. Por exemplo, para exibir uma lista de comandos do SysRq, pressione h.

```
[ec2-user ~]$ h
```

O comando h gera algo semelhante ao seguinte.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw/filesystems(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unwind(r) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-buffer(z)
```

## SSH client

### Para usar o SysRq em um cliente SSH

1. [Connect \(p. 1630\)](#) (Conecte-se) ao console serial da instância.
2. Para enviar uma solicitação de interrupção, pressione ~B (til, seguido de maiúsculas B).

```
[ec2-user ~]$ ~B
```

3. Para emitir um comando do SysRq, pressione a tecla no teclado que corresponde ao comando requerido. Por exemplo, para exibir uma lista de comandos do SysRq, pressione h.

```
[ec2-user ~]$ h
```

O comando h gera algo semelhante ao seguinte.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw/filesystems(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unwind(r) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-buffer(z)
```

## Note

O comando que você usa para enviar uma solicitação de interrupção pode ser diferente, dependendo do cliente SSH que você está usando.

## 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.

É possível enviar uma interrupção para diagnóstico a uma instância do Linux inacessível ou sem resposta para acionar manualmente um pânico de kernel.

Os sistemas operacionais Linux normalmente falham e reinicializam quando ocorre um pânico de kernel. O comportamento específico do sistema operacional depende de sua configuração. Um pânico de kernel também pode ser usado para fazer com que o kernel do sistema operacional da instância execute tarefas, como a geração de um arquivo de despejo de falha. Você pode usar as informações no arquivo de despejo da falha para conduzir uma análise de causa raiz e depurar a instância.

Os dados do despejo da falha 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 \(p. 1641\)](#)
- [Prerequisites \(p. 1641\)](#)
- [Enviar uma interrupção para diagnóstico \(p. 1643\)](#)

## 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 \(p. 210\)](#).

## Prerequisites

Antes de usar uma interrupção para diagnóstico, configure o sistema operacional da instância. Isso garante que ele desempenhe as funções necessárias quando ocorrer um pânico de kernel.

Para configurar o Amazon Linux 2 para gerar um despejo de falha quando ocorrer um pânico de kernel

1. Conecte-se à sua instância.
2. Instale kexec e kdump.

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. Configure o kernel para reservar uma quantidade de memória para o kernel secundário. A quantidade de memória a ser reservada depende da memória disponível total de sua instância. Abra o arquivo `/etc/default/grub` usando o editor de texto de sua preferência, localize a linha que começa com `GRUB_CMDLINE_LINUX_DEFAULT` e adicione o parâmetro `crashkernel` no seguinte formato: `crashkernel=memory_to_reserve`. Por exemplo, para reservar 160MB, modifique o arquivo `grub` da seguinte forma:

```
GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=160M console=tty0 console=ttyS0,115200n8
net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
rd.shell=0"
GRUB_TIMEOUT=0
GRUB_DISABLE_RECOVERY="true"
```

4. Salve as alterações e feche o arquivo `grub`.
5. Recompile o arquivo de configuração do GRUB2.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Em instâncias com base em processadores Intel e AMD, o comando `send-diagnostic-interrupt` envia uma interrupção não mascarável (NMI - non-maskable interrupt) desconhecida para a instância. É necessário configurar o kernel para falhar quando receber a NMI desconhecida. Abra o arquivo `/etc/sysctl.conf` usando o editor de texto de sua preferência e adicione o seguinte.

```
kernel.unknown_nmi_panic=1
```

7. Reinicialize e reconecte-se a sua instância.
8. Verifique se o kernel foi inicializado com o parâmetro `crashkernel` correto.

```
$ grep crashkernel /proc/cmdline
```

A saída do seguinte exemplo indica uma configuração bem-sucedida.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-e38f-408e-878b-fed395b47ad6 ro crashkernel=160M console=tty0 console=ttyS0,115200n8 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0
```

9. Verifique se o serviço kdump está em execução.

```
[ec2-user ~]$ systemctl status kdump.service
```

A saída do seguinte exemplo mostrará o resultado se o kdump estiver em execução.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset: enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
     Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
    Main PID: 2503 (code=exited, status=0/SUCCESS)
```

### Note

Por padrão, o arquivo de dump da falha é salvo em `/var/crash/`. Para alterar o local, modifique o arquivo `/etc/kdump.conf` usando o editor de texto de sua preferência.

Para configurar o Amazon Linux para gerar um despejo de falha quando ocorrer um pânico de kernel

1. Conecte-se à sua instância.
2. Instale kexec e kdump.

```
[ec2-user ~]$ sudo yum install kexec-tools -y
```

3. Configure o kernel para reservar uma quantidade de memória para o kernel secundário. A quantidade de memória a ser reservada depende da memória disponível total de sua instância.

```
$ sudo grub2 --args="crashkernel=memory_to_reserve" --update-kernel=ALL
```

Por exemplo, para reservar 160MB para o kernel de falha, use o seguinte comando.

```
$ sudo grubpy --args="crashkernel=160M" --update-kernel=ALL
```

4. Em instâncias com base em processadores Intel e AMD, o comando `send-diagnostic-interrupt` envia uma interrupção não mascarável (NMI - non-maskable interrupt) desconhecida para a instância. É necessário configurar o kernel para falhar quando receber a NMI desconhecida. Abra o arquivo `/etc/sysctl.conf` usando o editor de texto de sua preferência e adicione o seguinte.

```
kernel.unknown_nmi_panic=1
```

5. Reinicialize e reconecte-se a sua instância.
6. Verifique se o kernel foi inicializado com o parâmetro `crashkernel` correto.

```
$ grep crashkernel /proc/cmdline
```

A saída do seguinte exemplo indica uma configuração bem-sucedida.

```
root=LABEL=/ console=tty1 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295  
LANG=en_US.UTF-8 KEYTABLE=us crashkernel=160M
```

7. Verifique se o serviço `kdump` está em execução.

```
[ec2-user ~]$ sudo service kdump status
```

Se o serviço estiver em execução, o comando retornará a resposta `Kdump is operational.`

#### Note

Por padrão, o arquivo de dump da falha é salvo em `/var/crash/`. Para alterar o local, modifique o arquivo `/etc/kdump.conf` usando o editor de texto de sua preferência.

Para configurar o SUSE Linux Enterprise, o Ubuntu ou o Red Hat Enterprise Linux

Consulte os seguintes sites:

- [SUSE Linux Enterprise](#)
- [Ubuntu](#)
- [Red Hat Enterprise Linux \(RHEL\)](#)

#### Note

Em instâncias com base em processadores Intel e AMD, o comando `send-diagnostic-interrupt` envia uma interrupção não mascarável (NMI - non-maskable interrupt) desconhecida para a instância. É necessário configurar o kernel para falhar quando receber a NMI desconhecida. Adicione o conteúdo a seguir ao arquivo de configuração:

```
kernel.unknown_nmi_panic=1
```

## 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
```

# 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
<a href="#">Reservas de Capacidade sob demanda e direcionadas para EC2 Fleet</a>	O EC2 Fleet pode iniciar Instâncias sob demanda nas Reservas de Capacidade <b>targeted</b> .	22 de setembro de 2021
<a href="#">Instâncias T3 em hosts dedicados</a>	Support para instâncias T3 no Host Dedicado Amazon EC2.	14 de setembro de 2021
<a href="#">Suporte de hibernação para RHEL, Fedora e CentOS</a>	Coloque em hibernação suas instâncias recém-iniciadas que foram iniciadas a partir de AMIs RHEL, Fedora e CentOS.	9 de setembro de 2021
<a href="#">Novas Local Zones adicionadas</a>	Adicionar Local Zones em Chicago, Minneapolis e Kansas City.	8 de setembro de 2021
<a href="#">Amazon EC2 Global View</a>	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
<a href="#">Suporte de defasagem de AMI para Amazon Data Lifecycle Manager</a>	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
<a href="#">Suporte à hibernação para C5d, M5d e R5d</a>	Coloque em hibernação suas instâncias recém-iniciadas em execução nos tipos de instância C5d, M5d e R5d.	19 de agosto de 2021
<a href="#">Pares de chave do Amazon EC2</a>	O Amazon EC2 agora é compatível com chaves ED25519 em instâncias Linux e Mac.	17 de agosto de 2021
<a href="#">Instâncias M6i (p. 1645)</a>	Novas instâncias de uso geral com processadores Intel Xeon escalável de terceira geração (Ice Lake).	16 de agosto de 2021

<a href="#">Métricas do CloudWatch para o Amazon Data Lifecycle Manager</a>	É possível monitorar suas políticas do Amazon Data Lifecycle Manager usando o Amazon CloudWatch.	28 de julho de 2021
<a href="#">Nova Local Zone adicionada</a>	Adicionar Local Zone em Denver.	27 de julho de 2021
<a href="#">Eventos de dados do CloudTrail para APIs diretas do EBS</a>	As APIs ListSnapshotBlocks, ListChangedBlocks, GetSnapshotBlock e PutSnapshotBlock podem ser eventos de dados registrados no CloudTrail.	27 de julho de 2021
<a href="#">Prefixos para interfaces de rede</a>	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
<a href="#">Volumes io2 do Block Express</a>	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
<a href="#">Janelas de eventos</a>	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
<a href="#">IDs de recursos e suporte a marcação para regras de grupo de segurança (p. 1645)</a>	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
<a href="#">Novas Local Zones adicionadas</a>	Adicionar Local Zones em Dallas e na Filadélfia.	7 de julho de 2021
<a href="#">Defasar uma AMI</a>	Agora você pode especificar quando uma AMI é defasada.	11 de junho de 2021
<a href="#">Cobrança do Windows por segundo (p. 1645)</a>	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
<a href="#">Reservas de Capacidade no AWS Outposts</a>	Agora você pode usar as Reservas de Capacidade no AWS Outposts.	24 de maio de 2021
<a href="#">Compartilhamento de reserva de capacidade</a>	Agora é possível compartilhar Reservas de Capacidade criadas em Local Zones e zonas do Wavelength.	24 de maio de 2021

<a href="#">Instâncias virtualizadas com mais memória (p. 1645)</a>	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
<a href="#">Substituição do volume raiz</a>	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
<a href="#">Armazenar e restaurar uma AMI usando o S3</a>	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
<a href="#">Console serial do EC2</a>	Solucionar problemas de inicialização e conectividade de rede estabelecendo uma conexão com a porta serial de uma instância.	30 de março de 2021
<a href="#">Modos de inicialização</a>	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
<a href="#">Instâncias X2gd (p. 1645)</a>	Novas instâncias otimizadas para memória com um processador AWS Graviton2 baseado na arquitetura Arm de 64 bits.	16 de março de 2021
<a href="#">Amazon EBS local snapshots on Outposts</a>	Agora você pode usar Snapshots locais do Amazon EBS em Outposts para armazenar snapshots de volumes em um Outpost localmente no Amazon S3 no próprio Outpost.	4 de fevereiro de 2021
<a href="#">Crie um registro de DNS reverso</a>	Agora você pode configurar a pesquisa de DNS reverso para os seus endereços IP elásticos.	3 de fevereiro de 2021
<a href="#">Suporte multianexo para volumes de io2</a>	Agora você pode habilitar SSD de IOPS provisionadas (io2) para Amazon EBS Multi-Attach.	18 de dezembro de 2020
<a href="#">Instâncias C6gn (p. 1645)</a>	Novas instâncias otimizadas para computação com um processador AWS Graviton2 baseado na arquitetura Arm de 64 bits. Essas instâncias podem utilizar até 100 Gbps de largura de banda de rede.	18 de dezembro de 2020

<a href="#">Amazon Data Lifecycle Manager</a>	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
<a href="#">Instâncias do G4ad (p. 1645)</a>	Novas instâncias alimentadas por GPUs AMD Radeon Pro V520 e processadores AMD EPYC de 2ª geração.	9 de dezembro de 2020
<a href="#">Marcar AMIs e snapshots na criação de AMI</a>	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
<a href="#">Visualização de io2 Block Express</a>	Agora você pode optar por participar da demonstração de volumes io2 Block Express. 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
<a href="#">volumes gp (p. 1645)</a>	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
<a href="#">Instâncias D3, D3en, M5zn e R5b (p. 1645)</a>	Novos tipos de instância criados no sistema Nitro.	1º de dezembro de 2020
<a href="#">Tamanhos de volume de disco rígido otimizado e disco rígido frio com taxa de transferência</a>	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
<a href="#">Instâncias Mac</a>	Novas instâncias criadas em minicomputadores Apple Mac compatíveis com a execução de workloads do macOS no Amazon EC2.	30 de novembro de 2020
<a href="#">Use o Amazon EventBridge para monitorar eventos de frota spot</a>	Crie regras do EventBridge que açãoem ações programáticas em resposta a alterações e erros de estado de frota spot.	20 de novembro de 2020
<a href="#">Use Amazon EventBridge para monitorar eventos de Frota do EC2</a>	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

<a href="#">Excluir frotas de instant</a>	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
<a href="#">Suporte de hibernação para T3 e T3a</a>	Hiberne suas instâncias recém-executadas em execução em tipos de instância T3 e T3a.	17 de novembro de 2020
<a href="#">Criação rápida do Amazon EFS</a>	Você pode criar e montar um sistema de arquivos Amazon Elastic File System (Amazon EFS) em uma instância durante a execução usando o Amazon EFS Quick Create.	9 de novembro de 2020
<a href="#">Amazon Data Lifecycle Manager</a>	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
<a href="#">Categoria de metadados da instância: eventos/recomendações/rebalanceamento</a>	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
<a href="#">Recomendação de rebalanceamento de instâncias do EC2</a>	Um sinal que o notifica quando uma instância spot está em risco elevado de interrupção.	4 de novembro de 2020
<a href="#">Reservas de Capacidade em zonas Wavelength</a>	Reservas de Capacidade agora podem ser criadas e usadas em zonas Wavelength.	4 de novembro de 2020
<a href="#">Rebalanceamento de capacidade</a>	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
<a href="#">Instâncias P4d (p. 1645)</a>	Novas instâncias de computação acelerada que fornecem uma plataforma de alta performance para machine learning e workloads de HPC.	2 de novembro de 2020
<a href="#">Suporte à hibernação para I3, M5ad e R5ad</a>	Hibernar suas instâncias recém-iniciadas em execução nos tipos de instância I3, M5ad e R5ad.	21 de outubro de 2020

<a href="#">Limites de vCPU da instância spot</a>	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
<a href="#">Reservas de Capacidade em Local Zones</a>	Reservas de Capacidade agora podem ser criadas e usadas em Local Zones.	30 de setembro de 2020
<a href="#">Amazon Data Lifecycle Manager</a>	As políticas do Amazon Data Lifecycle Manager podem ser configuradas com até quatro programações.	17 de setembro de 2020
<a href="#">Instâncias T4g (p. 1645)</a>	As novas instâncias de uso geral desenvolvidas por processadores AWS Graviton2, que são baseados em núcleos Arm Neoverse de 64 bits e silício personalizado desenvolvidos pela AWS para fornecer níveis otimizados de performance e custo.	14 de setembro de 2020
<a href="#">Suporte à hibernação para M5a e R5a</a>	Hiberne suas instâncias recém-executadas em execução nos tipos de instância M5a e R5a.	28 de agosto de 2020
<a href="#">Volumes SSD de IOPS provisionadas (io2) para Amazon EBS</a>	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
<a href="#">Os metadados da instância fornecem informações de posicionamento e localização da instância</a>	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
<a href="#">Instâncias C5ad (p. 1645)</a>	Novas instâncias otimizadas para computação com processadores AMD EYPC de segunda geração.	13 de agosto de 2020
<a href="#">Zonas do Wavelength</a>	Uma Wavelength Zone é uma zona isolada no local da transportadora em que a infraestrutura de Wavelength é implantada.	6 de agosto de 2020

<a href="#">Grupos de Reserva de capacidade</a>	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
<a href="#">Instâncias C6gd, M6gd e R6gd (p. 1645)</a>	As novas instâncias de uso geral desenvolvidas por processadores AWS Graviton2, que são baseados em núcleos Arm Neoverse de 64 bits e silício personalizado desenvolvidos pela AWS para fornecer níveis otimizados de performance e custo.	27 de julho de 2020
<a href="#">Restauração rápida de snapshots</a>	Você pode habilitar a restauração rápida de snapshots compartilhados com você.	21 de julho de 2020
<a href="#">Instâncias C6g e R6g (p. 1645)</a>	As novas instâncias de uso geral desenvolvidas por processadores AWS Graviton2, que são baseados em núcleos Arm Neoverse de 64 bits e silício personalizado desenvolvidos pela AWS para fornecer níveis otimizados de performance e custo.	10 de junho de 2020
<a href="#">Instâncias bare metal para G4dn (p. 1645)</a>	Novas instâncias que fornecem aos aplicativos acesso direto aos recursos físicos do servidor de host.	5 de junho de 2020
<a href="#">Instâncias C5a (p. 1645)</a>	Novas instâncias otimizadas para computação com processadores AMD EYPC de segunda geração.	4 de junho de 2020
<a href="#">Traga seus próprios endereços IPv</a>	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
<a href="#">Instâncias M6g (p. 1645)</a>	As novas instâncias de uso geral desenvolvidas por processadores AWS Graviton2, que são baseados em núcleos Arm Neoverse de 64 bits e silício personalizado desenvolvidos pela AWS para fornecer níveis otimizados de performance e custo.	11 de maio de 2020

<a href="#">Executar instâncias usando um parâmetro do Systems Manager</a>	Você pode especificar um parâmetro do AWS Systems Manager em vez de uma AMI ao executar uma instância.	5 de maio de 2020
<a href="#">Personalizar notificações de eventos programados</a>	É possível personalizar notificações de eventos programados para incluir tags na notificação por e-mail.	4 de maio de 2020
<a href="#">Kernel Live Patching para Amazon Linux</a>	O Kernel Live Patching para Amazon Linux 2 permite que você aplique vulnerabilidades de segurança e patches de erros críticos a um kernel do Linux em execução, sem reinicializações ou interrupções a aplicativos de execução.	28 de abril de 2020
<a href="#">Multi-Attach do Amazon EBS</a>	Agora você pode anexar um único volume SSD de IOPS provisionadas (io1) a até 16 instâncias baseadas em Nitro que estejam na mesma zona de disponibilidade.	14 de fevereiro de 2020
<a href="#">Interromper e iniciar uma instância spot</a>	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
<a href="#">Marcação de recursos (p. 1645)</a>	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
<a href="#">Conectar-se à sua instância usando o Gerenciador de sessões</a>	Você pode iniciar uma sessão do Gerenciador de sessões com uma instância no console do Amazon EC2.	18 de dezembro de 2019
<a href="#">Instâncias Inf (p. 1645)</a>	Novas instâncias apresentando o AWS Inferentia, um chip de inferência de machine learning projetado para fornecer alta performance com economia.	3 de dezembro de 2019
<a href="#">Hosts dedicados e grupos de recursos de host</a>	Hosts dedicados agora podem ser usados com grupos de recursos de host.	2 de dezembro de 2019

<a href="#">Compartilhamento de Host dedicado</a>	Agora é possível compartilhar os hosts dedicados entre contas da AWS.	2 de dezembro de 2019
<a href="#">Especificação de crédito padrão no nível da conta</a>	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
<a href="#">Descoberta de tipo de instância</a>	Você pode encontrar um tipo de instância que atenda às suas necessidades.	22 de novembro de 2019
<a href="#">Dedicated Hosts (p. 1645)</a>	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
<a href="#">Restaurações rápidas de snapshots do Amazon EBS</a>	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
<a href="#">Instance Metadata Service Version 2</a>	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
<a href="#">Elastic Fabric Adapter (p. 1645)</a>	O Adaptador de malha elástica agora pode ser usado com a Intel MPI 2019 Update 6.	15 de novembro de 2019
<a href="#">Compras na fila de Instâncias reservadas</a>	É possível colocar a compra de uma Instância reservada na fila até três anos de maneira antecipada.	4 de outubro de 2019
<a href="#">Instâncias do G4dn (p. 1645)</a>	Novas instâncias com GPUs NVIDIA Tesla.	19 de setembro de 2019
<a href="#">Interrupção para diagnóstico</a>	É possível enviar uma interrupção para diagnóstico a uma instância inacessível ou sem resposta para acionar um pânico de kernel.	14 de agosto de 2019

<a href="#">Estratégia de alocação otimizada por capacidade</a>	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
<a href="#">Compartilhamento do Reservas de capacidade sob demanda</a>	Agora é possível compartilhar as Reservas de Capacidade entre contas da AWS.	29 de julho de 2019
<a href="#">Elastic Fabric Adapter (p. 1645)</a>	O EFA agora oferece suporte à Open MPI 3.1.4 e à Intel MPI 2019 Update 4.	26 de julho de 2019
<a href="#">Marcação de recursos (p. 1645)</a>	Executar modelos na criação.	24 de julho de 2019
<a href="#">EC2 Instance Connect</a>	O EC2 Instance Connect é uma forma simples e segura de conectar-se com suas instâncias usando Secure Shell (SSH).	27 de junho de 2019
<a href="#">Recuperação do host</a>	Reinicie automaticamente suas instâncias em um novo host no caso de uma falha inesperada do hardware em um Host dedicado.	5 de junho de 2019
<a href="#">Snapshots de vários volumes do Amazon EBS</a>	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
<a href="#">Marcação de recursos (p. 1645)</a>	Você pode marcar Reservas de hosts dedicados.	27 de maio de 2019
<a href="#">Criptografia por padrão do Amazon EBS</a>	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
<a href="#">Marcação de recursos (p. 1645)</a>	É possível marcar VPC endpoints, serviços de endpoint e configurações do serviço de endpoint.	13 de maio de 2019
<a href="#">Assistente de realocação de plataformas Windows para Linux para bancos de dados do Microsoft SQL Server</a>	Mover workloads existentes do Microsoft SQL Server de um sistema operacional Windows para Linux.	8 de maio de 2019

<a href="#">Instâncias I3en (p. 1645)</a>	As novas instâncias I3en podem utilizar até 100 Gbps de largura de banda de rede.	8 de maio de 2019
<a href="#">Elastic Fabric Adapter</a>	Você pode anexar um Elastic Fabric Adapter às suas instâncias para acelerar os aplicativos High Performance Computing (HPC).	29 de abril de 2019
<a href="#">Instâncias T3a (p. 1645)</a>	Novas instâncias com processadores AMD EYPC.	24 de abril de 2019
<a href="#">Instâncias M5ad e R5ad (p. 1645)</a>	Novas instâncias com processadores AMD EYPC.	27 de março de 2019
<a href="#">Marcação de recursos (p. 1645)</a>	Você pode atribuir tags personalizadas às reservas de Host dedicado para categorizá-las de diferentes maneiras.	14 de março de 2019
<a href="#">Instâncias bare metal para M5, M5d, R5, R5d e z1d (p. 1645)</a>	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 <a href="#">Placement groups de partição (p. 1086)</a> .	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
Hibernar instâncias do EC2 do Linux	15/11/2016	É possível hibernar uma instância do Linux se ela estiver habilitada para hibernação e atender aos pré-requisitos de hibernação. Para obter mais informações, consulte <a href="#">Hibernar a instância do Windows sob demanda ou reservada (p. 566)</a> .	28 de novembro de 2018
Amazon Elastic Inference Accelerators	15/11/2016	É possível anexar um Amazon EI Accelerator a suas instâncias para adicionar aceleração da plataforma de GPU para reduzir o custo de inferência de deep learning. Para obter mais informações, consulte <a href="#">Amazon Elastic Inference (p. 698)</a> .	28 de novembro de 2018

Recurso	Versão da API	Descrição	Data de lançamento
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
Instâncias com processadores baseados em Arm	15/11/2016	As novas instâncias A1 fornecem economias de custo significativas e são ideais para workloads expandidas e baseadas em Arm.	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 <a href="#">Criar uma solicitação de frota spot (p. 764)</a> .	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 <a href="#">Tipos de solicitação da Frota do EC2 (p. 702)</a> .	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 <a href="#">Economia na compra das Instâncias spot (p. 397)</a> .	5 de novembro de 2018
Supporte 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 <a href="#">Optimizar as opções de CPU (p. 616)</a> .	31 de outubro de 2018
Supporte 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 <a href="#">Criar um modelo de execução (p. 519)</a> .	30 de outubro de 2018

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">On-Demand Capacity Reservations (p. 481)</a> .	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 <a href="#">Traga seus próprios endereços IP (BYOIP) no Amazon EC2 (p. 954)</a> .	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 <a href="#">Alocar Hosts dedicados (p. 446)</a> .	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 <a href="#">Instâncias otimizadas para memória (p. 282)</a> .	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 <a href="#">Alterar a escala da frota spot usando a escalabilidade programada (p. 785)</a> .	20 de setembro de 2018
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 <a href="#">Instâncias expansíveis (p. 228)</a> .	21 de agosto de 2018

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Estratégias de alocação para Instâncias spot (p. 721)</a> .	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 <a href="#">Estratégia de alocação para Instâncias spot (p. 750)</a> .	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 <a href="#">Instâncias otimizadas para memória (p. 282)</a> .	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 <a href="#">Instâncias otimizadas para memória (p. 282)</a> .	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 <a href="#">Amazon Data Lifecycle Manager (p. 1359)</a> .	12 de julho de 2018
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 <a href="#">Criar um modelo de execução (p. 519)</a> .	11 de julho de 2018
Marcação de Hosts dedicados	15/11/2016	Você pode marcar seus Hosts dedicados. Para obter mais informações, consulte <a href="#">Marcação de Hosts dedicados (p. 458)</a> .	3 de julho de 2018

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Instâncias otimizadas para armazenamento (p. 297)</a> .	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 <a href="#">get-console-output</a> 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 <a href="#">Otimizar as opções de CPU (p. 616)</a> .	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 <a href="#">EC2 Fleet (p. 700)</a> .	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 <a href="#">Frota spot (p. 749)</a> .	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 <a href="#">Criar snapshots de Amazon EBS (p. 1307)</a> .	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 <a href="#">Alterar o placement group de uma instância (p. 1094)</a> .	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 <a href="#">IDs de recursos (p. 1543)</a> .	9 de fevereiro de 2018
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 <a href="#">Recursos de redes e armazenamento (p. 211)</a> .	24 de janeiro de 2018
Marcar endereços IP elásticos	15/11/2016	Você pode marcar seus endereços IP elásticos. Para obter mais informações, consulte <a href="#">Aplicar uma tag em um endereço IP elástico (p. 978)</a> .	21 de dezembro de 2017

Recurso	Versão da API	Descrição	Data de lançamento
Amazon Linux 2	15/11/2016	O Amazon Linux 2 é uma nova versão do Amazon Linux. Ele proporciona uma base de alta performance, estável e segura para suas aplicações. Para obter mais informações, consulte <a href="#">Amazon Linux (p. 172)</a> .	13 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 <a href="#">Definir o horário da sua instância do Linux (p. 610)</a> .	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 <a href="#">Instâncias expansíveis (p. 228)</a> .	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 <a href="#">Executar uma instância a partir de um modelo de execução (p. 517)</a> .	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 <a href="#">Placement groups de distribuição (p. 1086)</a> .	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 <a href="#">Instâncias otimizadas para armazenamento (p. 297)</a> .	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 <a href="#">Hibernar Instâncias spot interrompida (p. 429)</a> .	28 de novembro de 2017
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 <a href="#">Alterar a escala da frota spot usando as políticas de monitoramento do objetivo (p. 782)</a> .	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

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Instâncias otimizadas para memória (p. 282)</a> .	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 <a href="#">Instâncias otimizadas para computação (p. 273)</a> .	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 <a href="#">Trocar Instâncias reservadas conversíveis (p. 383)</a> .	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 <a href="#">Linux Instâncias computacionais aceleradas do (p. 305)</a> .	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 <a href="#">Alterar a locação de uma VPC (p. 481)</a> .	16 de outubro de 2017
Cobrança por segundo	15/11/2016	O Amazon EC2 cobra por segundo pela utilização baseada em Linux, com uma cobrança mínima de um minuto.	2 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 <a href="#">Comportamentos de interrupção (p. 428)</a> .	18 de setembro de 2017
Marcar gateways NAT	15/11/2016	Você pode marcar o gateway NAT. Para obter mais informações, consulte <a href="#">Marcar com tag os recursos do (p. 1553)</a> .	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 <a href="#">Regras de grupos de segurança (p. 1226)</a> .	31 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 <a href="#">Recuperar um endereço IP elástico (p. 982)</a> .	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

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Linux Instâncias computacionais aceleradas</a> (p. 305).	13 de julho de 2017
Instâncias F1	15/11/2016	As instâncias F1 são instâncias de computação aceleradas. Para obter mais informações, consulte <a href="#">Linux Instâncias computacionais aceleradas</a> (p. 305).	19 de abril 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 <a href="#">Marcar com tag os recursos</a> (p. 1553). 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, <a href="#">Conceder permissão para marcar recursos durante a criação</a> (p. 1144).	28 de março de 2017
Instâncias I3	15/11/2016	As instâncias I3 são instâncias otimizadas para armazenamento. Para obter mais informações, consulte <a href="#">Instâncias otimizadas para armazenamento</a> (p. 297).	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 <a href="#">Volumes elásticos do Amazon EBS</a> (p. 1405).	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 <a href="#">Funções do IAM para Amazon EC2</a> (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 <a href="#">Especificar uma locação para suas Instâncias spot</a> (p. 401).	19 de janeiro de 2017
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 <a href="#">Endereçamento IP de instâncias do Amazon EC2</a> (p. 937).	1º de dezembro de 2016

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Instâncias otimizadas para memória (p. 282)</a>	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 intermitência 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 <a href="#">Instâncias expansíveis (p. 228)</a> .	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 <a href="#">Linux Instâncias computacionais aceleradas (p. 305)</a> .	29 de setembro de 2016
m4.16xlarge	01/04/2016	Instâncias 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 <a href="#">Escalabilidade automática para frota spot (p. 780)</a> .	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 <a href="#">Suporte a redes avançadas (p. 1016)</a> .	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 <a href="#">IDs de recursos (p. 1543)</a> .	23 de junho de 2016
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 <a href="#">Copiar um snapshot do Amazon EBS. (p. 1313)</a> .	21 de junho de 2016

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Fazer uma captura de tela de uma instância inacessível (p. 1610)</a> .	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 <a href="#">Instâncias otimizadas para memória (p. 282)</a> .	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 <a href="#">Tipos de volume do Amazon EBS (p. 1253)</a> .	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 <a href="#">Métricas de instância (p. 876)</a> .	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 <a href="#">Métricas do CloudWatch para frota spot (p. 778)</a> .	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 <a href="#">Scheduled Reserved Instances (p. 387)</a> .	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 <a href="#">IDs de recursos (p. 1543)</a> .	13 de janeiro de 2016
Suporte 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 <a href="#">Habilitar o suporte a DNS do ClassicLink (p. 1115)</a> .	11 de janeiro de 2016

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Instâncias expansíveis (p. 228)</a> .	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 <a href="#">Dedicated Hosts (p. 440)</a> .	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 <a href="#">Definir uma duração para suas Instâncias spot (p. 401)</a> .	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 <a href="#">Modificar uma solicitação de frota spot (p. 775)</a> .	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 <a href="#">Estratégia de alocação para Instâncias spot (p. 750)</a> .	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 <a href="#">Peso de instâncias de frotas spot (p. 756)</a> .	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 <a href="#">Criar alarmes para interromper, encerrar, reiniciar ou recuperar uma instância (p. 898)</a> .	23 de julho de 2015

Recurso	Versão da API	Descrição	Data de lançamento
Novo tipo de instância <code>t2.large</code>		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 <a href="#">Instâncias expansíveis (p. 228)</a> .	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 <a href="#">Frota spot (p. 749)</a> .	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 <a href="#">Migrar um endereço IP elástico do EC2-Classic (p. 1106)</a> .	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 <a href="#">Como importar uma VM como uma imagem usando o VM Import/Export</a> no Guia do usuário de VM Import/Export.	23 de abril de 2015
Novo tipo de instância <code>g2.8xlarge</code>		A nova instância <code>g2.8xlarge</code> 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/performace 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 <a href="#">Instâncias otimizadas para armazenamento (p. 297)</a>.</p>	24 de março 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 <a href="#">Recuperar a instância (p. 593)</a>.</p>	12 de janeiro de 2015
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. Expandido 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 <a href="#">Instâncias otimizadas para computação (p. 273)</a>.</p>	11 de janeiro de 2015

Recurso	Versão da API	Descrição	Data de lançamento
ClassicLink	01/10/2014	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 <a href="#">ClassicLink (p. 1109)</a> .	7 de janeiro de 2015
Notificações de encerramento de instância spot		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.  Para obter mais informações, consulte <a href="#">Avisos de interrupção de instância spot (p. 432)</a> .	5 de janeiro de 2015
DescribeVolumesSupport à paginação de	01/09/2014	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 <a href="#">DescribeVolumes</a> no Amazon EC2 API Reference.	23 de outubro 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 <a href="#">Instâncias expansíveis (p. 228)</a> .	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 <a href="#">Volumes de Finalidade geral (SSD) (gp2) (p. 1256)</a> .	16 de junho 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 <a href="#">Criptografia de Amazon EBS (p. 1418)</a> .	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 <a href="#">Amazon EC2 Instance Types</a> (Tipos de instância do Amazon EC2).	9 de abril de 2014
Nova versão da AMI do Amazon Linux		A AMI do Amazon Linux 2014.03 está liberada.	27 de março 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 <a href="#">Relatórios de uso do Amazon EC2 (p. 1567)</a> .	28 de janeiro de 2014
Instâncias M3 adicionais	15/10/2013	Os tamanhos de instâncias M3 <code>m3.medium</code> e <code>m3.large</code> agora são compatíveis. Para obter mais informações sobre as especificações de hardware de cada tipo de instância do Amazon EC2, consulte <a href="#">Amazon EC2 Instance Types</a> (Tipos de instância do Amazon EC2).	20 de janeiro de 2014

Recurso	Versão da API	Descrição	Data de lançamento
Instâncias I2	15/10/2013	Essas instâncias fornecem IOPS muito altos e oferecem suporte a TRIM em instâncias do Linux para melhor performance de gravações sucessivas de SSD. 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 <a href="#">Instâncias otimizadas para armazenamento (p. 297)</a> .	19 de dezembro de 2013
Instâncias M3 atualizadas	15/10/2013	Os tamanhos de instâncias M3, <code>m3.xlarge</code> e <code>m3.2xlarge</code> , agora oferecem suporte ao armazenamento de instâncias com volumes SSD.	19 de dezembro de 2013
Importação de máquinas virtuais do Linux	15/10/2013	O processo de VM Import agora oferece suporte à importação de instâncias do Linux. Para obter mais informações, consulte o <a href="#">VM Import/Export User Guide (Manual do usuário para importação/exportação de VMs)</a> .	16 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 <a href="#">Identity and Access Management para o Amazon EC2 (p. 1136)</a> .	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 <a href="#">Amazon EC2 Instance Types</a> (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 <a href="#">Executar uma instância AWS Marketplace (p. 533)</a> .	11 de novembro de 2013

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Linux Instâncias computacionais aceleradas (p. 305)</a> .	4 de novembro de 2013
Novo assistente de execução		Há um novo assistente de execução reprojetado do EC2. Para obter mais informações, consulte <a href="#">É possível executar uma instância usando o assistente de execução de instância. (p. 510)</a> .	10 de outubro de 2013
Modificação de tipos de instâncias reservadas do Amazon EC2	01/10/2013	Agora você pode modificar o tipo de instância de instâncias reservadas do Linux dentro da mesma família (por exemplo, M1, M2, M3, C1). Para obter mais informações, consulte <a href="#">Modificar a Instâncias reservadas (p. 375)</a> .	09 de outubro de 2013
Nova versão da AMI do Amazon Linux		A AMI do Amazon Linux 2013.09 está liberada.	30 de setembro de 2013
Modificação de instâncias reservadas do Amazon EC2	15/08/2013	Agora você pode modificar instâncias reservadas em uma região. Para obter mais informações, consulte <a href="#">Modificar a Instâncias reservadas (p. 375)</a> .	11 de setembro de 2013
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 <a href="#">Atribuir um endereço IPv4 público durante a execução da instância (p. 942)</a> .	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 <a href="#">Políticas do IAM no Amazon EC2 (p. 1139)</a> .	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 <a href="#">Copiar um snapshot do Amazon EBS. (p. 1313)</a> .	11 de junho de 2013
Nova página Tags		Há uma nova página Tags no console do Amazon EC2. Para obter mais informações, consulte <a href="#">Marcar com tag os recursos do Amazon EC2 (p. 1552)</a> .	04 de abril de 2013
Nova versão da AMI do Amazon Linux		A AMI do Amazon Linux 2013.03 está liberada.	27 de março de 2013

Recurso	Versão da API	Descrição	Data de lançamento
Tipos de instâncias otimizadas para EBS adicionais	01/02/2013	<p>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>.</p> <p>Para obter mais informações, consulte <a href="#">Instâncias otimizadas para Amazon EBS (p. 1438)</a>.</p>	19 de março de 2013
Cópia de uma AMI de uma região para outra	01/02/2013	<p>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.</p> <p>Para obter mais informações, consulte <a href="#">Copiar um AMI (p. 144)</a>.</p>	11 de março de 2013
Execução de instâncias em uma VPC padrão	01/02/2013	<p>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.</p>	11 de março de 2013
Tipo de instância em cluster ( <code>cr1.8xlarge</code> ) com mais memória	01/12/2012	<p>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.</p>	21 de janeiro de 2013
Tipo de instância de alto armazenamento ( <code>hs1.8xlarge</code> )	01/12/2012	<p>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.</p>	20 de dezembro de 2012
Cópia de snapshot do EBS	01/12/2012	<p>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 <a href="#">Copiar um snapshot do Amazon EBS. (p. 1313)</a>.</p>	17 de dezembro de 2012
Verificações de métricas e status do EBS atualizadas para volumes do Provisioned IOPS SSD	01/10/2012	<p>Atualizadas as métricas do EBS para incluir duas novas métricas para volumes do Provisioned IOPS SSD. Para obter mais informações, consulte <a href="#">Métricas do Amazon CloudWatch para o Amazon EBS (p. 1477)</a>. Novas verificações de status também adicionadas para volumes do Provisioned IOPS SSD. Para obter mais informações, consulte <a href="#">Verificações de status do volume do EBS (p. 1292)</a>.</p>	20 de novembro de 2012

Recurso	Versão da API	Descrição	Data de lançamento
Kernels do Linux		IDs de AKI atualizados; kernels de distribuição reorganizados; seção de PVOps atualizada.	13 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 <a href="#">Amazon EC2 Instance Types</a> (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
Nova versão da AMI do Amazon Linux		A AMI do Amazon Linux 2012.09 está liberada.	11 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
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 <a href="#">Tipos de volume do Amazon EBS (p. 1253)</a> .	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:	11 de junho de 2012
		<ul style="list-style-type: none"> <li>• Chaves de acesso da AWS para aplicações que executam em instâncias do Amazon EC2.</li> <li>• Rotação automática das chaves de acesso da AWS na instância do Amazon EC2.</li> <li>• Permissões granulares para aplicações que executam em instâncias do Amazon EC2 que fazem solicitações para seus serviços da AWS.</li> </ul>	

Recurso	Versão da API	Descrição	Data de lançamento
Os recursos de instâncias spot que facilitam a familiarização e o manuseio de possíveis interrupções.		<p>Agora é possível gerenciar suas Instâncias spot da seguinte forma:</p> <ul style="list-style-type: none"> <li>• 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 <a href="#">Como executar Instâncias spot no grupo do Auto Scaling</a> no Guia do usuário do Amazon EC2 Auto Scaling.</li> <li>• Obter notificações quando as instâncias forem executadas ou encerradas.</li> <li>• Usar modelos do AWS CloudFormation para executar instâncias spot em uma pilha com recursos da AWS.</li> </ul>	7 de junho de 2012
Exportação de instâncias do EC2 e time stamps para verificações de status para o Amazon EC2	01/05/2012	Supporte 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
Exportação de instâncias do EC2 e time stamps em verificações do status de instâncias e do sistema para a Amazon VPC	01/05/2012	<p>Supporte adicionado para a exportação de instâncias do EC2 ao Citrix Xen, ao Microsoft Hyper-V e ao VMware vSphere.</p> <p>Supporte adicionado para time stamps em verificações de status de instâncias e do sistema.</p>	25 de maio de 2012
Instância óctupla extragrande de computação em cluster	01/04/2012	Supporte adicionado para instâncias <code>cc2.8xlarge</code> 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
Nova versão da AMI do Linux		A AMI do Amazon Linux 2012.03 está liberada.	28 de março de 2012
Nova versão da AKI		Liberamos a versão 1.03 da AKI e as AKIs para a região AWS GovCloud (US) .	28 de março de 2012
Instâncias médias, suporte para 64 bits em todas as AMIs e um cliente SSH baseado em Java	15/12/2011	Supporte adicionado para um novo tipo de instância e informações 64 bits. Procedimentos adicionados para usar o cliente SSH baseado em Java para conexão a instâncias Linux.	7 de março de 2012

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Interfaces de rede elástica (p. 984)</a> .	21 de dezembro de 2011
Nova região e AKIs de GRU		Adicionadas informações sobre a versão de novas AKIs para a região SA-East-1. Essa versão desativa o AKI versão 1.01. O AKI versão 1.02 continuará sendo compatível com versões anteriores.	14 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 <a href="#">Monitorar o status das instâncias (p. 841)</a> .	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
Nova região e AKIs de PDX		Adicionadas informações sobre a versão de novas AKIs para a nova região US-West 2.	8 de novembro de 2011
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

Recurso	Versão da API	Descrição	Data de lançamento
Nova versão da AMI do Linux		Adição de informações sobre a versão do Amazon Linux AMI 2011.09. Essa atualização remove a tag beta da AMI do Amazon Linux, oferece suporte à capacidade de bloquear os repositórios em uma versão específica, e fornece notificações quando atualizações estão disponíveis para pacotes instalados incluindo atualizações de segurança.	26 de setembro 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 <a href="#">VM Import/Export User Guide (Manual do usuário para importação/exportação de VMs)</a> .	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
Habilitação da AMI do Linux para executar kernels fornecidos pelo usuário		Adição de informações sobre a alteração da versão do AKI de 1.01 para 1.02. Esta versão atualiza o PVGRUB para lidar com falhas de execução associadas a instâncias do Linux t1.micro. Para obter mais informações, consulte <a href="#">Enabling Your Own Linux Kernels (p. 191)</a> .	20 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 <a href="#">Identity and Access Management para o Amazon EC2 (p. 1136)</a> .	26 de abril de 2011
Habilitação da AMI do Linux para executar kernels fornecidos pelo usuário		Adicionadas informações sobre como habilitar uma AMI do Linux para usar a Amazon Kernel Image (AKI) para executar um kernel fornecido pelo usuário. Para obter mais informações, consulte <a href="#">Enabling Your Own Linux Kernels (p. 191)</a> .	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 <a href="#">Dedicated Instances (p. 475)</a> .	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. Para obter mais informações, consulte <a href="#">Reserved Instances (p. 343)</a> .	27 de março de 2011
Nova AMI de referência do Amazon Linux		A nova AMI de referência do Amazon Linux substitui a AMI de referência do CentOS. Removidas as informações sobre a AMI de referência do CentOS incluindo a seção nomeada Correção do descompasso do clock para instâncias em cluster na AMI do CentOS 5.4.	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 <a href="#">Metadados da instância e dados do usuário (p. 649)</a> e <a href="#">Categorias de metadados da instância (p. 667)</a> .	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

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Desanexar um volume do Amazon EBS de uma instância Linux (p. 1300)</a> .	23 de fevereiro de 2011
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 <a href="#">Habilitar a proteção contra encerramento (p. 589)</a> .	23 de fevereiro de 2011
Correção do descompasso do clock para instâncias em cluster na AMI do CentOS 5.4		Adicionadas informações sobre como corrigir o descompasso do clock para instâncias em cluster em execução na AMI do CentOS 5.4.	25 de janeiro 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 <a href="#">VM Import/Export User Guide (Manual do usuário para importação/exportação de VMs)</a> .	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 <a href="#">Listar e filtrar seus recursos (p. 1544)</a> e <a href="#">Marcar com tag os recursos do Amazon EC2 (p. 1552)</a> .	19 de setembro de 2010
Execução de instância idempotente	31/08/2010	Adicionadas informações sobre garantia de idempotência ao executar instâncias. Para obter mais informações, consulte <a href="#">Como garantir idempotência</a> no Amazon EC2 API Reference.	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 <a href="#">Instâncias expansíveis (p. 228)</a> .	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 <a href="#">Identity and Access Management para o Amazon EC2 (p. 1136)</a> .	2 de setembro de 2010

Recurso	Versão da API	Descrição	Data de lançamento
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 <a href="#">Amazon EC2 Instance Types</a> (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 <a href="#">Métricas do Amazon CloudWatch para o Amazon EBS (p. 1477)</a> .	14 de junho de 2010
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 <a href="#">Amazon EC2 Instance Types</a> (Tipos de instância do Amazon EC2).	22 de fevereiro de 2010